

American Furukawa, Inc. v. Hossain, --- F.Supp.3d ---- (2015)

2015 IER Cases 182,599

2015 WL 2124794
Only the Westlaw citation is currently available.
United States District Court,
E.D. Michigan,
Southern Division.

AMERICAN FURUKAWA, INC., Plaintiff,

v.

Isthihar HOSSAIN, Defendant.

Case No. 14-cv-13633. | Signed May 6, 2015.

Synopsis

Background: Employer brought action against former employee, alleging that employee unlawfully accessed its computers to obtain confidential information in violation of the Computer Fraud and Abuse Act (CFAA), and asserting claims under Michigan law for fraud, breach of contract, breach of fiduciary duty, misappropriation of trade secrets, and conversion. Employee moved for partial judgment on the pleadings.

Holdings: The District Court, Gershwin A. Drain, J., held that:

^[1] employer properly alleged that employee took computer files “without authorization,” in violation of CFAA;

^[2] employer properly alleged that employee “exceeded authorized access” in order to take computer files, in violation of CFAA;

^[3] Michigan Uniform Trade Secrets Act (MUTSA) did not preempt employer’s claims for fraud, breach of contract, breach of fiduciary duty, and conversion;

^[4] employer’s policies and practices handbook, which explicitly noted that adoption of the handbook was entirely voluntary and should not be construed as creating a contractual relationship, did not warrant dismissal of employer’s breach of contract claim; and

^[5] employer properly alleged conversion claim under Michigan law.

Motion denied.

West Headnotes (10)

^[1] **Federal Civil Procedure**

⚡ Judgment on the Pleadings

170AFederal Civil Procedure
170AVIIPleadings
170AVII(L)Judgment on the Pleadings
170AVII(L)In General
170Ak1041In general

Federal courts review motions for judgment on the pleadings using the standards applicable to motions to dismiss for failure to state a claim. Fed.Rules Civ.Proc.Rule 12(b)(6), (c), 28 U.S.C.A.

Cases that cite this headnote

^[2] **Telecommunications**

⚡ Fraud; unauthorized access or transmission

372Telecommunications
372VIIIComputer Communications
372k1339Civil Liabilities; Illegal or Improper Purposes
372k1342Fraud; unauthorized access or transmission

Employer properly alleged that former employee took computer files “without authorization,” in violation of the Computer Fraud and Abuse Act (CFAA), based on allegations that employee accessed some computer files during leave of absence when he was told not to work for employer. 18 U.S.C.A. § 1030(a)(1–7).

4 Cases that cite this headnote

^[3] **Statutes**

⚡ Liberal or strict construction; rule of lenity

361Statutes
361IIIConstruction
361III(K)Particular Classes of Statutes, Construction

American Furukawa, Inc. v. Hossain, --- F.Supp.3d ---- (2015)

2015 IER Cases 182,599

of
 361k1316Penal Statutes
 361k1318Liberal or strict construction; rule of lenity

If a statute is not ambiguous, the use of canons of construction, reference to legislative history, and application of the rule of lenity is not appropriate.

Cases that cite this headnote

[4]

Telecommunications

⚡Fraud; unauthorized access or transmission

372Telecommunications
 372VIIIComputer Communications
 372k1339Civil Liabilities; Illegal or Improper Purposes
 372k1342Fraud; unauthorized access or transmission

Employer properly alleged that former employee "exceeded authorized access" in order to take computer files, in violation of the Computer Fraud and Abuse Act (CFAA), based on allegations that employee accessed files in violation of employer's computer policy. 18 U.S.C.A. § 1030(a)(1-7).

4 Cases that cite this headnote

[5]

Antitrust and Trade Regulation

⚡Actions

Conversion and Civil Theft

⚡In general; nature and scope of remedy

Fraud

⚡Nature and form of remedy

Labor and Employment

⚡Preemption

29TAntitrust and Trade Regulation
 29TIVTrade Secrets and Proprietary Information
 29TIV(B)Actions
 29Tk426In general
 97CConversion and Civil Theft
 97CIActions
 97CII(A)Right of Action and Defenses
 97Ck120In general; nature and scope of remedy
 184Fraud
 184IIActions

184II(A)Rights of Action and Defenses
 184k31Nature and form of remedy
 231HLabor and Employment
 231HVIntellectual Property Rights and Duties
 231Hk303Preemption

Michigan Uniform Trade Secrets Act (MUTSA) did not preempt employer's claims against former employee under Michigan law for, inter alia, fraud, breach of contract, breach of fiduciary duty, and conversion, as employer's claims were not based solely on trade secrets. M.C.L.A. § 445.1908.

1 Cases that cite this headnote

[6]

Antitrust and Trade Regulation

⚡Actions

29TAntitrust and Trade Regulation
 29TIVTrade Secrets and Proprietary Information
 29TIV(B)Actions
 29Tk426In general

Michigan Uniform Trade Secrets Act (MUTSA) preempts claims based solely upon the misappropriation of a trade secret; conversely, where a cause of action exists in the commercial area not dependent on trade secrets, that cause continues to exist. M.C.L.A. § 445.1908.

1 Cases that cite this headnote

[7]

Labor and Employment

⚡Particular cases

231HLabor and Employment
 231HIIn General
 231Hk49Manuals, Handbooks, and Policy Statements
 231Hk51Particular cases

Employer's policies and practices handbook, which explicitly noted that adoption of the handbook was entirely voluntary on the part of the company and should not be construed as creating a contractual relationship between the company and any employee, did not warrant dismissal of employer's claim against former employee for breach of contract under Michigan

American Furukawa, Inc. v. Hossain, --- F.Supp.3d ---- (2015)

2015 IER Cases 182,599

law, as the claim was not premised on the handbook, rather, the claim was only premised on employee's invention assignment and secrecy agreement and, impliedly, employer's removable media policy.

Cases that cite this headnote

97Ck108Assertion of ownership or control in general

In Michigan, conversion arises from any distinct act of domain wrongfully exerted over another's personal property in denial of or inconsistent with the rights therein.

Cases that cite this headnote

[8]

Contracts

⚙️Ambiguity in general

95Contracts

95IIConstruction and Operation

95II(A)General Rules of Construction

95k176Questions for Jury

95k176(2)Ambiguity in general

In Michigan, if contract language is clear and unambiguous, its meaning is a question of law.

Cases that cite this headnote

Attorneys and Law Firms

Joseph J. Vogan, Varnum, Riddering, Grand Rapids, MI, Brett A. Rendeiro, Varnum, Riddering, Novi, MI, for Plaintiff.

Jason M. Shinn, Shinn Legal, PLC, Keego Harbor, MI, for Defendant.

OPINION AND ORDER DENYING DEFENDANT'S MOTION FOR PARTIAL JUDGMENT ON THE PLEADINGS [30]

GERSHWIN A. DRAIN, District Judge.

I. INTRODUCTION

*1 American Furukawa, Inc. ("Furukawa" or "Plaintiff") commenced the instant action against its former employee, Istihar Hossain ("Defendant"), on September 19, 2014. *See* Dkt. No. 1. In the Complaint, Furukawa alleges that Hossain unlawfully accessed its computers to obtain confidential information in violation of the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030. Additionally, Furukawa brings claims under Michigan law for Fraud, Breach of Contract, Breach of Fiduciary Duty, Misappropriation of Trade Secrets, and Conversion. *Id.*

When it filed the Complaint, Furukawa simultaneously moved for a Temporary Restraining Order ("TRO"). *See* Dkt. No. 4. On September 22, 2014, the Court entered a TRO enjoining Hossain from using Furukawa's information, and ordering Hossain to show cause why a preliminary injunction should not be issued; account for

[9]

Conversion and Civil Theft

⚙️Title and Right to Possession of Plaintiff

97CConversion and Civil Theft

97CIIActions

97CII(A)Right of Action and Defenses

97Ck123Title and Right to Possession of Plaintiff

97Ck124In general

Employer properly alleged conversion claim under Michigan law against former employee, based on allegation that employee took information from employer's servers, even though some of the information pertained to third parties unrelated to employer.

Cases that cite this headnote

[10]

Conversion and Civil Theft

⚙️Assertion of ownership or control in general

97CConversion and Civil Theft

97CIAActs Constituting and Liability Therefor

American Furukawa, Inc. v. Hossain, --- F.Supp.3d ---- (2015)

2015 IER Cases 182,599

and return Furukawa's confidential information; and abide by a confidentiality agreement between the parties. *See* Dkt. No. 7. The parties entered a Stipulated Order leaving the terms of the TRO in place, while setting forth an agreed protocol for examining the computers and email accounts at issue. *See* Dkt. No. 18.

Presently before the Court is Defendant's Partial Motion for Judgment on the Pleadings Pursuant to Rule 12(c) of the Federal Rules of Civil Procedure. *See* Dkt. No. 30. Furukawa filed a Response to Hossain's Motion, but Hossain failed to file a Reply in accordance with the Court's Local Rules. *See* E.D. Mich. L.R. 7.1(e)(1)(c). After reviewing the briefing, the Court concludes that oral argument will not aid in the resolution of this matter. Accordingly, the Court will resolve the Motion on the briefs as submitted. *See* E.D. Mich. L.R. 7.1(f)(2). For the reasons discussed herein, the Court will **DENY** Hossain's Motion for Partial Judgment on the Pleadings Pursuant to Rule 12(c) of the Federal Rules of Civil Procedure [30].

II. FACTUAL BACKGROUND

American Furukawa, Inc. is a Delaware corporation and its principal place of business is located at 47677 Galleon Ct, Plymouth, Michigan. Furukawa is a supplier of advanced technology automotive, electronics and specialty products to several high technology industries. Istihar Hossain accepted employment with Furukawa in September, 2011 as a Power Systems Electrical Engineer. Hossain reported to Furukawa's General Manager and Vice President.

When Hossain began his employment with Furukawa, Furukawa asserts that Hossain agreed to abide by Furukawa's Policies regarding "Supplier and Vendor Information," "Conflicts of Interest," "Confidentiality," "Outside Employment," "Company Property" and "Removable Media Use." Furukawa also asserts that Hossain entered into an Invention Assignment & Secrecy Agreement ("Secrecy Agreement") with Furukawa, which dictated that Hossain "will regard and preserve as confidential all trade secrets pertaining to the Company's business that have been or may be obtained by me by reason of my employment." The Secrecy Agreement also dictated that Hossain would not "without prior authority from the Company to do so, use for my own benefit or purposes, nor disclose to others, either during my employment or thereafter" any trade secrets pertaining to Furukawa's business.

*2 By 2014, Hossain had become a Production Manager and Senior Production Manager with access to Furukawa's trade secrets, know-how, intellectual property and other confidential information. On March 11, 2014, while he was still employed by Furukawa, Furukawa asserts that Hossain entered into an "Employment Agreement" ("Agreement") with Huatong—a competitor and supplier to Furukawa. As part of Hossain's alleged Agreement with Huatong, Hossain was to serve as CEO of a new sales company, American Huatong. Also on March 11, Furukawa asserts that Hossain downloaded 910 Furukawa files to his external hard drive without his manager's permission.

On March 14, 2014, Furukawa states that Hossain called into Furukawa's offices and indicated he was sick. Yet, on March 17, 2014, Furukawa asserts that Hossain downloaded another 875 Furukawa files and also moved two-and-a-half years of email from Furukawa's exchange server to his external hard drive without his manager's permission. While files were allegedly being downloaded on March 17, 2014, Furukawa states that Hossain informed Furukawa he was unable to work due to a basketball injury. Notably, pursuant to his alleged Agreement with Huatong, Hossain was scheduled to begin his employment with Huatong on March 17, 2014.

As a result of his reported injury, Hossain was granted a leave of absence, commencing March 18, 2014. Critically, as a condition for granting the leave of absence, Furukawa asserts that it instructed Hossain that he could not do "any work" for Furukawa during his leave of absence. Despite the instructions to the contrary, Furukawa asserts that Hossain accessed information on his company laptop and copied Furukawa files from his company email to his personal "gmail" account during his leave of absence. Furukawa purportedly did not learn of Hossain's activities until the following chain of events raised suspicion.

On March 20, 2014, Huatong announced that it would no longer sell Electrical Submersible Pump ("ESP") cables to the United States market through a partnership with Furukawa. Huatong also announced that it would no longer sell service drop cables to Kingwire, and photovoltaic ("PV") cables to the United States market, through Furukawa.

On Thursday, April 24, 2014, Hossain sent an email to Furukawa's Manager of Human Resources stating that his doctor had cleared him to return to work. On April 25, 2014, Furukawa claims Hossain reported for work late and left early. On Monday, April 28, 2014, Hossain announced that he was resigning his employment, effective May 2, 2014. Furukawa accepted Hossain's

American Furukawa, Inc. v. Hossain, --- F.Supp.3d ---- (2015)

2015 IER Cases 182,599

resignation, effective April 29, 2014, and paid him through May 2, 2014.

Despite his alleged Agreement with Huatong, when he resigned his employment, Hossain allegedly indicated he did not “have another job lined up or anything,” but his “previous employer” had been contacting him, and he was “pretty sure” that he could get a job with them. Upon his departure from Furukawa, Hossain was asked to sign an “Employee Certification & Agreement on Termination,” certifying that he had returned all property belonging to the Company, had complied with the Secrecy Agreement and would continue to abide by that Agreement. Hossain allegedly refused to sign.

*3 On or about May 12, 2014, Furukawa learned that Huatong had approached WTEC—one of Furukawa’s customers—about buying cable from Huatong. On May 16, 2014, Furukawa received an email from WTEC regarding WTEC’s “compound” requirements and “payment terms.” The email from WTEC was addressed to Hossain at his former Furukawa email address. On May 30, 2014, WTEC confirmed that Hossain was acting as Huatong’s agent with respect to the sales negotiations between WTEC and Huatong. On June 5, 2014, Furukawa received another email from WTEC, addressed to Hossain’s Furukawa email address purportedly asking Hossain to quote the price for “PV Wire 2kV AL S-8000” and “PV Wire 2kV CU.”

Furukawa sent a letter to Hossain on June 9, 2014, reminding him of his obligations under the Secrecy Agreement. In the letter, Furukawa demanded that Hossain immediately cease and desist from any further solicitation of cable business from WTEC or any other customer of Furukawa. Furukawa also sought assurances that Hossain would abide by his trade secret obligations, and would not use or disclose any trade secret information that he acquired during his employment with Furukawa. Hossain purportedly refused to comply with this request. Furukawa attempted to negotiate with Hossain to resolve the dispute. Throughout the negotiations, Hossain purportedly maintained that he had returned all property belonging to Furukawa and fully complied with the Secrecy Agreement. After looking into the actions of Hossain, Furukawa brought the instant action pursuant to the CFAA and Michigan law.

III. DISCUSSION

A. LEGAL STANDARD

^[1] Federal courts review motions for judgment on the pleadings brought pursuant to Federal Rule of Civil Procedure 12(c) using the standards applicable to motions filed under Rule 12(b)(6). See *Wee Care Child Ctr., Inc. v. Lumpkin*, 680 F.3d 841, 846 (6th Cir.2012). Though litigants employ these procedural mechanisms at different stages of the proceedings, the purpose of both motions is to test the legal sufficiency of a plaintiff’s pleadings. Thus, as with Rule 12(b)(6) motions, a Rule 12(c) motion allows a court to make an assessment as to whether a plaintiff has stated a claim upon which relief can be granted. Fed.R.Civ.P. 12(b)(6).

As articulated by the Supreme Court of the United States, “[t]o survive a motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to ‘state a claim to relief that is plausible on its face.’ ” *Ashcroft v. Iqbal*, 556 U.S. 662, 678, 129 S.Ct. 1937, 173 L.Ed.2d 868 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570, 127 S.Ct. 1955, 167 L.Ed.2d 929 (2007)). This facial plausibility standard requires claimants to put forth “enough fact[s] to raise a reasonable expectation that discovery will reveal evidence of” the requisite elements of their claims. *Twombly*, 550 U.S. at 557, 127 S.Ct. 1955. Even though a complaint need not contain “detailed” factual allegations, its “factual allegations must be enough to raise a right to relief above the speculative level.” *Ass’n of Cleveland Fire Fighters v. City of Cleveland*, 502 F.3d 545, 548 (6th Cir.2007) (citing *Twombly*, 550 U.S. at 555, 127 S.Ct. 1955) (internal citations omitted).

*4 While courts are required to accept the factual allegations in a complaint as true, *Twombly*, 550 U.S. at 556, 127 S.Ct. 1955, the presumption of truth does not apply to a claimant’s legal conclusions, *Iqbal*, 556 U.S. at 678, 129 S.Ct. 1937. Therefore, to survive a motion to dismiss, a plaintiff’s pleading for relief must provide “more than labels and conclusions, and a formulaic recitation of the elements of a cause of action will not do.” *Ass’n of Cleveland Fire Fighters*, 502 F.3d at 548 (quoting *Twombly*, 550 U.S. at 555, 127 S.Ct. 1955) (internal citations and quotations omitted).

In addition to evaluating the sufficiency of the factual allegations within the four corners of a complaint, courts may consider any exhibits attached to the complaint, matters of public record, and exhibits attached to a defendant’s 12(b)(6) motion, provided that the latter are referred to in the complaint and are central to the claims therein. See *Bassett v. NCAA*, 528 F.3d 426, 430 (6th Cir.2008) (citing *Amini v. Oberlin Coll.*, 259 F.3d 493, 502 (6th Cir.2001)).

American Furukawa, Inc. v. Hossain, --- F.Supp.3d ---- (2015)

2015 IER Cases 182,599

B. LEGAL ANALYSIS

The central question presented by Hossain's Motion is whether this Court should adopt the approach taken by other district courts in Michigan to find that Hossain did not violate the CFAA when he removed files from Furukawa servers in contravention of a confidentiality agreement and computer policy.

The Court must also resolve the following questions presented by Hossain's Motion: whether the Michigan Uniform Trade Secrets Act ("MUTSA") preempts Furukawa's claims for Fraud, Breach of Contract, Breach of Fiduciary Duty, and Conversion; whether Furukawa's Breach of Contract claim is precluded by disclaimer language in the Furukawa Policies and Practices Handbook; and whether Furukawa can bring a claim for Conversion.

With respect to the central question advanced in Hossain's Motion, the Court navigated a deep circuit split regarding interpretations of the CFAA's phrases "without authorization" and "exceeds authorized access." The Sixth Circuit has given separate meaning to both of these phrases. Following the Sixth Circuit's guidance, this Court finds that Furukawa has stated a proper claim under the CFAA, because Furukawa has plead that Hossain accessed some files when he was told not to work for Furukawa—"without authorization"—and accessed other files in violation of a computer policy—"exceeds authorized access."

With respect to the remaining questions presented by Hossain's Motion, the Court finds that Furukawa's claims under Michigan law are not preempted by MUTSA because Furukawa's claims are not based *solely* on trade secrets. Additionally, the Court finds that Furukawa's Breach of Contract claim is not premised on the Furukawa Policies and Practices Handbook, so the handbook does not warrant the dismissal of Furukawa's claim. Lastly, the Court finds that Furukawa has presented a proper claim for Conversion because Hossain took information from Furukawa's servers. The Court's findings are addressed in detail below.

1. Furukawa Properly Asserts Claims Under the CFAA

*5 The CFAA prohibits seven types of conduct involving unauthorized access to computers. *See* 18 U.S.C. § 1030(a)(1)-(7). While the CFAA was initially just a criminal statute, in 1994 Congress added private civil causes of action to permit "[a]ny person who suffers damage or loss by reason of a violation of [the statute]" to "maintain a civil action against the violator to obtain

compensatory damages and injunctive relief or other equitable relief." 18 U.S.C. § 1030(g).

Furukawa contends that Hossain violated 18 U.S.C. § 1030(a)(2)(C) ("Subsection (a)(2)(C) of the CFAA"), which imputes liability to anyone who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains ... information from any protected computer." 18 U.S.C. § 1030(a)(2)(C). Additionally, Furukawa asserts that Hossain violated 18 U.S.C. § 1030(a)(4) ("Subsection (a)(4) of the CFAA"), which imputes liability to anyone who "knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value [.]" 18 U.S.C. § 1030(a)(4).

Under both Subsection (a)(2)(C) and Subsection (a)(4) of the CFAA, Hossain would be liable if Furukawa is able to demonstrate that he accessed a "protected computer" either "without authorization" or in a manner that "exceeds authorized access." However, Furukawa must also show that it suffered "damage"² or "loss"³ as a result of Hossain's purported violation of the CFAA, and must demonstrate that the purported violation involved at least one of five aggravating factors "set forth in subclauses (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i)." 18 U.S.C. § 1030(g). Only one factor is relevant to the present claim: 18 U.S.C. § 1030(c)(4)(A)(i)(I), which requires the showing of "loss to 1 or more persons during any 1-year period ... aggregating at least \$5,000 in value." 18 U.S.C. § 1030(c)(4)(A)(i)(I).

Thus, to set forth a proper civil claim under the CFAA based on a violation of Subsection (a)(2), Furukawa must show that Hossain: (1) intentionally accessed a computer, (2) without authorization or exceeding authorized access, and that he (3) thereby obtained information (4) from any protected computer (if the conduct involved an interstate or foreign communication), and that (5) there was loss to one or more persons during any one-year period aggregating at least \$5,000 in value. *See LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1132 (9th Cir.2009).

To successfully bring an action under the CFAA based on a violation of Subsection (a)(4), Furukawa must show that Hossain: (1) accessed a "protected computer," (2) without authorization or exceeding such authorization that was granted, (3) "knowingly" and with "intent to defraud," and thereby (4) "further [ed] the intended fraud and obtain[ed] anything of value," causing (5) a loss to one or more persons during any one-year period aggregating at least \$5,000 in value. *See id.* (citing *P.C. Yonkers, Inc. v. Celebrations the Party and Seasonal Superstore, LLC*, 428 F.3d 504, 508 (3d Cir.2005)).

American Furukawa, Inc. v. Hossain, --- F.Supp.3d ---- (2015)

2015 IER Cases 182,599

*6 Here, Hossain contends that he is entitled to partial judgment on the pleadings because Furukawa cannot satisfy the first and second factors of either of these inquiries. In other words, Hossain contends that Furukawa cannot show he accessed a protected computer either “without authorization” or in a manner that “exceeds authorized access.” The Court disagrees.

The CFAA does not define the phrase “without authorization,” however the CFAA does define “exceeds authorized access” as follows: “[T]o access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter.” 18 U.S.C. § 1030(e)(6). Given the similarity of the phrases, there is a deep circuit split regarding interpretations and the scope of the CFAA. The circuit split has been cast as a clash between “broad” and “narrow” interpretations of the CFAA’s phrases “without authorization” and “exceeds authorized access.”

The “broad” approach was first adopted by the First Circuit, which found that an employee “exceeds authorized access” by violating a confidentiality agreement. *See EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 581–84 (1st Cir.2001). Later, the Seventh Circuit adopted a “broad” view based on principles of agency when it found that an employee acted “without authorization” as soon as the employee severed the agency relationship through disloyal activity. *See Int’l Airport Ctrs., LLC v. Citrin*, 440 F.3d 418 (7th Cir.2006).

More recently, however, courts have moved away from a “broad” view premised on theories of agency and violations of confidentiality agreements. The more recent trend for the “broad” approach finds that an employee “exceeds authorized access” by violating employer policies regarding access and use of computers. *See, e.g., United States v. John*, 597 F.3d 263, 271–73 (5th Cir.2010) (“While we do not necessarily agree that violating a confidentiality agreement ... would give rise to criminal culpability, we do agree with the First Circuit that the concept of ‘exceeds authorized access’ may include exceeding the purposes for which access is ‘authorized.’ ”); *United States v. Rodriguez*, 628 F.3d 1258, 1263 (11th Cir.2010); *EF Cultural Travel BV v. Zefer Corp.*, 318 F.3d 58, 62 (1st Cir.2003) (“A lack of authorization could be established by an explicit statement [.]”); *see also United States v. Salum*, 257 Fed.Appx. 225, 230 (11th Cir.2007); *United States v. Teague*, 646 F.3d 1119, 1121–22 (8th Cir.2011).

The Ninth Circuit was the first Circuit to adopt the “narrow” interpretation of the CFAA by narrowly interpreting the CFAA’s “without authorization”

language. *See LVRC Holdings LLC v. Brekka*, 581 F.3d 1127 (9th Cir.2009). In so doing, the Ninth Circuit repudiated the “broad” approach, which used principles of agency to give meaning to the CFAA’s “without authorization” language. *See Brekka*, 581 F.3d at 1134. The Court in *Brekka* explicitly refused to hold an employee liable under the CFAA’s “without authorization” language based on an agency theory in order to avoid interpreting the CFAA in a “surprising and novel way[] that impose[s] unexpected burdens on defendants.” *Brekka*, 581 F.3d at 1134.

*7 Instead, the Ninth Circuit in *Brekka* advanced what it deemed a “sensible” interpretation of the CFAA, giving separate meaning to the phrases “without authorization” and “exceeds authorized access” by focusing on “the employer’s decision to allow or to terminate an employee’s authorization to access a computer[.]” *Brekka*, 581 F.3d at 1133. In so doing, the *Brekka* decision adopted a “narrow” approach when giving meaning to the CFAA’s “without authorization” language. However, to give meaning to the CFAA’s “exceeds authorized access” language, the *Brekka* Court simply applied the definition provided by Congress. Under the analysis put forth by the court in *Brekka*, whether an individual “exceeds authorized access” “depends on the actions taken by the employer.” *Brekka*, 581 F.3d at 1135.

In *Pulte Homes, Inc. v. Laborers’ International Union of North America*, the Sixth Circuit relied heavily on the *Brekka* decision to give meaning to the CFAA’s “without authorization” and “exceeds authorized access” language. 648 F.3d 295 (6th Cir.2011). In *Pulte Homes*, the Sixth Circuit found that the phrases were separate and distinct. *See Pulte Homes*, 648 F.3d at 304 (citing *Citrin*, 440 F.3d at 420, to note “that ‘the difference ... is paper thin,’ ” and citing *Daniel v. Cantrell*, 375 F.3d 377, 383 (6th Cir.2004), to note that the Sixth Circuit can give meaning to both “without authorization” and “exceeds authorized access” under the CFAA).

The Sixth Circuit relied on the *Brekka* decision to apply a “narrow” interpretation to the CFAA’s “without authorization” language. *See Pulte Homes*, 648 F.3d at 303–04. However, after recognizing a distinction between the CFAA’s phrases, the Sixth Circuit did not go beyond the CFAA’s provided definition to give meaning to “exceeds authorized access,” opting instead to simply apply the meaning provided by Congress, just as the Ninth Circuit did in *Brekka*. *See Pulte Homes*, 648 F.3d at 304; *cf. Brekka*, 581 F.3d at 1135. Essentially, the Sixth Circuit adopted the original “sensible” interpretation put forth by the Ninth Circuit’s *Brekka* decision.

American Furukawa, Inc. v. Hossain, --- F.Supp.3d ---- (2015)

2015 IER Cases 182,599

Nevertheless, the Ninth and Fourth Circuits later widened the circuit split by applying the “narrow” interpretation to give meaning to the CFAA’s “exceeds authorized access” language as well. See *United States v. Nosal*, 676 F.3d 854 (9th Cir.2012) (en banc); *WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199 (4th Cir.2012). Under the Ninth and Fourth Circuit’s new “narrow” interpretation of “exceeds authorized access,” an employee given access to a computer is authorized to access the computer regardless of any policies that regulate the use of the computer or its information. See *Nosal*, 676 F.3d at 863–64; *WEC Carolina*, 687 F.3d at 207.

Hossain argues that the approach taken by the Ninth and Fourth Circuits is proper because they interpret both the phrases “without authorization” and “exceeds authorized access” narrowly. Hossain urges this Court to follow other district courts in Michigan that have followed the Ninth and Fourth Circuit’s new “narrow” approach. See, e.g., *Ajuba Int’l, L.L.C. v. Saharia*, 871 F.Supp.2d 671 (E.D.Mich.2012); *Dana Ltd. v. Am. Axle & Mfg. Holdings, Inc.*, No. 1:10–CV–450, 2012 WL 2524008 (W.D.Mich. June 29, 2012).

*8 However, this Court is not bound by such decisions. See *Camreta v. Greene*, — U.S. —, 131 S.Ct. 2020, 2033 n. 7, 179 L.Ed.2d 1118 (2011). This Court must take its guidance from the Sixth Circuit, which interpreted the CFAA’s “without authorization” and “exceeds authorized access” language separately to give meaning to each phrase. See *Pulte Homes*, 648 F.3d at 303–04.

While “[d]ifferent interpretations of the same statute within the same district court are generally not preferred (except, perhaps, by courts of appeals, which were created in part to resolve such differences of opinion) [,]” *Dice Corp. v. Bold Technologies*, No. 11–13578, 2012 WL 263031, at *7 (E.D.Mich. Jan. 30, 2012), this Court will follow the guidance of the Sixth Circuit to find that a “narrow” interpretation is warranted to give meaning to the CFAA’s “without authorization” language, but not “exceeds authorized access.”

a. Without Authorization

The Court agrees with the other courts in this district who have adopted the “narrow” approach to give meaning to the CFAA’s “without authorization” language. In light of the meaning the Sixth Circuit gave to the phrase “without authorization,” this Court finds that adopting the “broad” agency approach advanced by Furukawa would be

contrary to plain meaning of the CFAA. Nevertheless, even under, the “narrow” approach, the Court finds that Furukawa has properly alleged that Hossain accessed some files “without authorization.”

i. The Sixth Circuit adopted a narrow interpretation of “without authorization,” which is controlling in this Court.

Furukawa pushes the Court to adopt a “broad” agency approach to give meaning to the CFAA’s “without authorization” language, arguing that “an employee accesses a computer ‘without authorization’ whenever the employee, without the employer’s knowledge, acquires an interest that is adverse to that of his employer or is guilty of a serious breach of loyalty.” Dkt. No. 33 at 18 (quoting *Guest-Tek Interactive Entm’t, Inc. v. Pullen*, 665 F.Supp.2d 42, 45 (D.Mass.2009)); see also *id.* (quoting *Citrin*, 440 F.3d at 420–21 to state: “The reasoning behind this approach is that ‘[v]iolating the duty of loyalty, or failing to disclose adverse interests, voids the agency relationship’ and, therefore, ‘terminates’ the agent’s ‘authority.’”).

This Court will not adopt a broad agency approach in light of the meaning the Sixth Circuit provided for the CFAA’s “without authorization” language. Because the CFAA’s “without authorization” language was not defined by Congress, the Sixth Circuit looked to term’s ordinary usage. See *Pulte Homes*, 648 F.3d at 303 (“Because Congress left the interpretation of ‘without authorization’ to the courts, we [] start with ordinary usage.”).

To define “authorization” the Sixth Circuit found that the “plain meaning of ‘authorization’ is ‘[t]he conferment of legality; ... sanction.’” *Id.* at 303–04 (citing 1 Oxford English Dictionary 798 (2d ed.1989)) (brackets in original). With this definition for “authorization,” the Sixth Circuit definitively concluded: “Commonly understood, then, a defendant who accesses a computer ‘without authorization’ does so *without sanction or permission*.” *Id.* (citing *Brekka*, 581 F.3d at 1132–33) (emphasis added).

*9 The Sixth Circuit’s definition of “without authorization” is in accord with other circuits that defined the term. For example, the Ninth Circuit explained that “a person who ‘intentionally accesses a computer without authorization,’ accesses a computer without any permission at all [.]” *Brekka*, 581 F.3d at 1133 (citing RANDOM HOUSE UNABRIDGED DICTIONARY, 139

American Furukawa, Inc. v. Hossain, --- F.Supp.3d ---- (2015)

2015 IER Cases 182,599

(2001) and WEBSTER'S THIRD INTERNATIONAL DICTIONARY, 146 (2002) to define "without authorization" (internal citations omitted); *cf. WEC Carolina*, 687 F.3d 199 at 204 (citing *Oxford English Dictionary* (2d ed.1989; online version 2012), to define " 'authorization' as 'formal warrant, or sanction[.]" and citing *Brekka*, 581 F.3d at 1133, to state an employee is " 'without authorization' when he gains admission to a computer without approval.").

While Furukawa argues that Hossain's authorization terminated with his alleged breach of the Secrecy Agreement, this Court disagrees. Just because an employee acquires interests adverse to their employer's, it does not inevitably follow that the employee accessed information "without authorization." Indeed, in *Brekka*—which the Sixth Circuit relies on heavily—the Ninth Circuit rejected such a "broad" agency based interpretation of the CFAA's "without authorization" language noting: "Nothing in the CFAA suggests that a defendant's liability for accessing a computer without authorization turns on whether the defendant breached a state law duty of loyalty to an employer." *Brekka*, 581 F.3d at 1135 (9th Cir.2009). This Court agrees, and will follow the guidance of the Sixth Circuit and interpret the CFAA's "without authorization" language narrowly. *See Pulte Homes*, 648 F.3d at 304.

ii. The rule of lenity requires a "narrow" interpretation of the CFAA's "without authorization" language.

Furukawa also argues "that the 'legislative history' supports the broad view." Dkt. No. 33 (citing *Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc.*, 119 F.Supp.2d 1121, 1127–29 (W.D.Wash.2000)). The *Brekka* court rejected a "broad" agency approach to avoid interpreting the CFAA's "without authorization" language in a "surprising and novel way[] that impose[d] unexpected burdens on defendants." *Brekka*, 581 F.3d at 1134 (citing *United States v. Santos*, 553 U.S. 507, 128 S.Ct. 2020, 170 L.Ed.2d 912 (2008) (J. Scalia) (plurality opinion)).

Because the CFAA is also a criminal statute, the Ninth Circuit emphasized that "[t]he rule of lenity, which is rooted in considerations of notice, requires courts to limit the reach of criminal statutes to the clear import of their text and construe any ambiguity against the government." *Id.* at 1135 (citing *United States v. Romm*, 455 F.3d 990, 1001 (9th Cir.2006)).

The Court in *Brekka* explained that unexpected results would follow if criminal liability were to turn on principles of agency. *See id.* ("If [an] employer has not rescinded the defendant's right to use the computer, the defendant would have no reason to know that making personal use of the company computer in breach of a state law fiduciary duty to an employer would constitute a criminal violation of the CFAA.")

***10** To avoid unexpected results with respect to interpreting "without authorization," the Ninth Circuit explicitly rejected the rational underpinning decisions finding liability under the CFAA based on an agency theory. *See Brekka*, 581 F.3d at 1135 (finding that the "interpretation [relied upon in] *Citrin* does not comport with the plain language of the CFAA, and given the care with which we must interpret criminal statutes to ensure that defendants are on notice as to which acts are criminal we decline to adopt the interpretation of 'without authorization' suggested by *Citrin*"). Again, this Court agrees with the Ninth Circuit's opinion in *Brekka*, and finds that the rule of lenity favors a narrow construction of the CFAA's "without authorization" language.

iii. Furukawa properly alleges that Hossain took some files "without authorization"

^[2] The Sixth Circuit provided the following guidance for determining whether an individual accesses information without authorization: "We ask [] whether [the defendant] had *any* right to call [the plaintiff's] offices and email its executives." *Id.* (emphasis in original). Following the guidance of the Sixth Circuit, this Court similarly asks whether Hossain had *any* right to access the Furukawa files. This Court finds Hossain did have a right up to a certain point.

In Furukawa's Complaint, it notes that "[i]n his capacity as Production manager and Senior Production Manager, Hossain had access to Furukawa's trade secrets, know-how, intellectual property or other confidential information [.]". Dkt. No. 1 at ¶ 30. Nonetheless, Furukawa claims Hossain illegally downloaded a total of 1,785 files to his external hard drive and two-and-half years of email from Furukawa's exchange server on March 10, 2014 and March 17, 2014.

Because Hossain had access on March 10, 2014 and March 17, 2014, the Court finds that the 1,785 files and the two-and-a-half years of email Hossain downloaded from Furukawa's exchange server were not downloaded "without authorization" under the CFAA. *Cf. Pulte*

American Furukawa, Inc. v. Hossain, --- F.Supp.3d ---- (2015)

2015 IER Cases 182,599

Homes, 648 F.3d at 304 (“Because [the plaintiff] does not allege that [the defendant] possessed *no* right to contact [the plaintiff’s] offices and its executives, it fails to satisfy one of the elements—access “without authorization”—of its claim.”) (emphasis in original).

Furukawa points to its Removable Media Policy to argue Hossain illegally accessed the files on March 11, 2014 and March 17, 2014. However, the Removable Media Policy is relevant in determining whether Hossain “exceeded authorized access,” on March 11, 2014 and March 17, 2014; not whether Hossain accessed the files “without authorization.” Hossain’s alleged disregard of the limitation put in place by the Removable Media Policy does not change the fact that Hossain was still authorized to access the files. *See Brekka*, 581 F.3d at 1133.⁴

Nevertheless, Furukawa does make a compelling point by noting that “[w]hile on leave of absence from his employment with Furukawa, [Hossain] also downloaded Furukawa’s files from his company computer to an external hard drive, and copied Furukawa’s files from his company email account to his personal ‘gmail’ account.” Dkt. No. 1 at ¶ 53.

*11 Furukawa highlights the fact that it informed Hossain he was not authorized to work during the period of March 18, 2014 to April 24, 2014. *See* Dkt. No. 33 at 21 (citing Dkt. No. 33–1 at 2–3). As a condition for granting the leave of absence, Furukawa instructed Hossain that he could not do “any work” for Furukawa during his leave of absence. *See* Dkt. No. 33 at 9. An interchange during Hossain’s deposition indicates that Hossain was verbally instructed he could not work for Furukawa, and that his access to his Furukawa email account and Furukawa’s network was physically revoked. Dkt. No. 1–1 (Deposition of Istihar Hossain).

In light of these facts, and assuming Furukawa’s allegations are true, the Court finds Hossain actually had *no* right to access files during his leave of absence. *See Pulte Homes*, 648 F.3d at 305; *see also Brekka*, 581 F.3d at 1136 (9th Cir.2009) (“There is no dispute that if [the defendant] accessed [the company’s] information ... after he left the company ..., [the defendant] would have accessed a protected computer ‘without authorization’ for purposes of the CFAA.”); *United States v. Steele*, 595 Fed.Appx. 208, 211 (4th Cir.2014) (“[T]he fact that [the defendant] no longer worked for [the company] when he accessed its server logically suggests that the authorization he enjoyed during his employment no longer existed.”).⁵

Accordingly, the Court finds that the 1,785 files and the two-and-a-half years of email Hossain downloaded to his external hard drive from Furukawa’s exchange server on March 10, 2014 and March 17, 2014 were *not* downloaded “without authorization” under the CFAA. However, because there were files allegedly downloaded without *any* permission during Hossain’s leave of absence, the Court finds that Hossain is not entitled to judgment on the pleadings for the CFAA claim as it pertains to accessing some files “without authorization.”

b. Exceeds Authorized Access

This Court will depart from the other district courts in Michigan that have found the Sixth Circuit favors a narrow approach to both the phrases “without authorization” and “exceeds authorized access.” This Court finds that the Sixth Circuit’s narrow approach does not extend to the CFAA’s “exceeds authorized access” language, because the Sixth Circuit relied on the unambiguous definition provided for the phrase. Accordingly, this Court finds that Furukawa properly alleged that Hossain “exceeded authorized access” by downloading Furukawa files in contravention of the Removable Media Policy.

i. The Sixth Circuit adopted the unambiguous definition of “exceeds authorized access” provided by Congress in the CFAA. Nothing in the definition provided by Congress forecloses employers from implementing computer policies that restrict both access and use.

As discussed, the Sixth Circuit recognized the distinction between the CFAA’s phrases “without authorization” and “exceeds authorized access.” *Pulte Homes*, 648 F.3d at 304 (citing *Citrin*, 440 F.3d at 420 and citing *Cantrell*, 375 F.3d at 383). This distinction is important because the Sixth Circuit’s opinion in *Pulte Homes* only adopted the “narrow” approach as it pertained to interpreting the phrase “without authorization,” not “exceeds authorized access.” *See Pulte Homes*, 648 F.3d at 304; *see also Dana Ltd.*, 2012 WL 2524008, at *3 (“[T]he Sixth Circuit’s opinion in *Pulte Homes*, suggests that the Sixth Circuit would adopt the narrow view insofar as it relied heavily on the ninth Circuit’s opinion in *LVRC Holdings* for a definition of ‘without authorization.’”) (emphasis added) (internal citation committed).

American Furukawa, Inc. v. Hossain, --- F.Supp.3d ---- (2015)

2015 IER Cases 182,599

*12 With respect to the phrase “exceeds authorized access,” the Sixth Circuit did not go beyond the plain language of the CFAA’s provided language. See *Pulte Homes*, 648 F.3d at 304 (citing 18 U.S.C. § 1030(e)(6) to note: “Unlike the phrase ‘without authorization,’ the CFAA helpfully defines ‘exceeds authorized access’”). The Sixth Circuit cited the Ninth Circuit’s opinion in *Brekka* to analyze the CFAA’s definition of “exceeds authorized access” and note: “Under this definition, ‘an individual who is authorized to use a computer for certain purposes but goes beyond those limitations ... has ‘exceed[ed] authorized access.’” *Pulte Homes*, 648 F.3d at 304 (quoting *Brekka*, 581 F.3d at 1133); cf. *Brekka*, 581 F.3d at 1133 (interpreting only the phrase “without authorization,” yet looking to the plain language of the phrase “exceeded authorized access” to reach “a sensible interpretation of §§ 1030(a)(2) and (4)[.]”).

The Sixth Circuit never indicated that limitations on employee access and use of employer computers were foreclosed by the CFAA. Thus, this Court disagrees with the court decisions cited by Hossain that take a “narrow” approach to the CFAA’s “exceeds authorized access” language in order to find that there can be no liability for an individual who violates a computer use policy. See, e.g., *Dana*, 2012 WL 2524008, at *4 (citing *Nosal*, 676 F.3d at 859, for the proposition that “[f]ederal criminal liability should not be based on every violation of a private computer use policy.”); *Ajuba*, 871 F.Supp.2d at 685–88 (narrowly interpreting “exceeds authorized access” to dismiss a CFAA claim where the employer alleged an employee exceeded his authorization by accessing computers in violation of use limitations).

The Ninth Circuit opinion from which the courts taking a narrow approach base their reasoning is out of step with the findings of the Sixth Circuit. While the Sixth Circuit simply looked to definition provided by Congress to interpret the CFAA’s “exceeds authorized access” language, the Ninth Circuit panel in *Nosal* looked beyond the definition provided by Congress to the legislative history of the CFAA to interpret the phrase. See *Nosal*, 676 F.3d at 860.

In *Nosal*, the United States (“the government”) sought to enforce a computer policy focused on access, purpose, and use. See Reply Brief for Petitioner Appellant, *United States v. Nosal*, 676 F.3d 854 (9th Cir.2012) (en banc) (No. 10–10038), 2010 WL 6191782, at *3. The government argued that the employees in *Nosal* were liable under the CFAA because the company “granted [the employees] a restricted right to access [the company] computers by explicitly instructing [the employees] to access information in the Searcher database only for legitimate [company] business purposes.” *Id.* at *3.

According to the government, “[w]hen [the employees] accessed the Searcher database for other purposes, they violated this express access restriction and thereby obtained proprietary [company] information that they were ‘not entitled so to obtain.’” *Id.* (citing 18 U.S.C. § 1030(e)(6)).

*13 The *Nosal* panel disagreed and found that “ ‘exceeds authorized access’ in the CFAA is limited to violations of restrictions on *access* to information, and not restrictions on its *use*.” *Nosal*, 676 F.3d at 864. To reach its decision, the *Nosal* panel claimed “to follow in the path blazed by *Brekka*[.]” *Id.* at 863. To the contrary, however, the *Nosal* panel parted from the path blazed by *Brekka* by refusing to emphasize the plain language of the CFAA and resorting to an unnecessary analysis of the CFAA’s legislative history. In so doing, the panel took “a plainly written statute and pars[ed] it in a hyper-complicated way that distort[ed] the obvious intent of Congress.” *United States v. Nosal*, 676 F.3d 854, 864 (9th Cir.2012) (Silverman, J., dissenting).

The *Nosal* panel ignored the “sensible interpretation of [the CFAA]” put forth in *Brekka* that relied on the plain language of the CFAA. See *Brekka*, 581 F.3d at 1133. In *Brekka*, the Ninth Circuit used the CFAA’s plain language to describe “a person who ‘exceeds authorized access’” as a person who “has permission to access the computer, but accesses information on the computer that *the person is not entitled to access*.” *Id.* (emphasis added).

As the government argued in *Nosal*, the operative term in the CFAA’s definition of “exceeds authorized access” is “entitled,” which is defined by *Webster’s New Riverside University Dictionary* as “to furnish with a right.” Brief for Petitioner Appellant, *United States v. Nosal*, 676 F.3d 854 (9th Cir.2012) (en banc) (No. 10–10038), 2010 WL 6191778, at *15 (citing *Webster’s New Riverside University Dictionary* 435). As the government explained, “[s]ince the employer furnishes the right to access its computer systems and obtain information from it, explicit policies restricting the right to obtain information from workplace computers determines when an individual ‘exceeds authorized access.’” *Id.*

The government further highlighted that the term “so” in definition provided for “exceeds authorized access” was defined as “[i]n the state or manner indicated or expressed.” Reply Brief for Petitioner Appellant, *United States v. Nosal*, 676 F.3d 854 (9th Cir.2012) (en banc) (No. 10–10038), 2010 WL 6191782, at *8 (quoting *Webster’s II New Riverside University Dictionary* 1102 (1988)). By noting that the provided definition of “exceeds authorized access” focused on *the manner* of access, the government explained that the provided

American Furukawa, Inc. v. Hossain, --- F.Supp.3d ---- (2015)

2015 IER Cases 182,599

definition means “someone exceeds authorized access when he obtains or alters information that he is not entitled to obtain or alter *in those circumstances*.” *Id.* (citing 18 U.S.C. § 1030(e)(6)) (emphasis in original).

Essentially, the government argued that the provided definition comports with the Sixth Circuit’s finding that “‘an individual who is authorized to use a computer for certain purposes *but goes beyond those limitations* ... has ‘exceed [ed] authorized access.’ ” *Pulte Homes*, 648 F.3d at 304 (quoting *Brekka*, 581 F.3d at 1133); *cf.* Reply Brief for Petitioner Appellant, 2010 WL 6191782, at *9 (“[T]he definition of ‘exceeds authorized access’ shows that someone exceeds authorized access by obtaining information *in a prohibited manner*, even if the accesser might be entitled to obtain the same information under other circumstances.”) (emphasis added).

*14 Nevertheless, the *Nosal* panel disagreed, finding that computer policies focused on use were “a poor fit with the statutory language [of the CFAA].” *Nosal*, 676 F.3d at 857. Instead, the *Nosal* panel found that in the provided definition of “exceeds authorized access,” “[a]n equally or more sensible reading of ‘entitled’ is as a synonym for ‘authorized.’ ” *Id.* The *Nosal* panel then found that the government placed “a great deal of weight on a two-letter word that is essentially a conjunction,” before finding that “the government’s ‘so’ argument [didn’t] work because the word has meaning even if it doesn’t refer to use restrictions.” *Nosal*, 676 F.3d at 857–58.

Thus, rather than address the government’s argument, which focused on the manner of access, the *Nosal* panel discounted the argument because it found “Congress could ... have included ‘so’ as a connector or for emphasis.” *Id.* at 858. This Court does not believe the Sixth Circuit would take the *Nosal* panel’s approach. By inflexibly focusing only on the government’s defining of the word “so,” the *Nosal* panel missed the overarching point that the government was attempting to make: that someone exceeds authorized access by obtaining information in a prohibited manner, even if the accesser might be entitled to obtain the same information under other circumstances. *See* Reply Brief for Petitioner Appellant, 2010 WL 6191782, at *9.

The *Nosal* panel seemed to imply that the manner in which an individual accesses information is inconsequential after providing the following hypothetical to explain why the government’s “so” argument purportedly didn’t work:

Suppose an employer keeps certain information in a separate database

that can be viewed on a computer screen, but not copied or downloaded. If an employee circumvents the security measures, copies the information to a thumb drive and walks out of the building with it in his pocket, he would then have obtained access to information in the computer that he is not “entitled *so* to obtain.”

Nosal, 676 F.3d at 858. However, in its hypothetical, the *Nosal* panel suggests that an employer is certainly able to bring an action against an individual under the CFAA if the individual accesses the employer’s computers in a manner that exceeds “security measures.”

This Court fails to see a difference between an employee who circumvents “security measures,” and an employee who circumvents explicit computer limitations provided by an employer for employees regarding the employee’s access, use, or purpose when accessing the employer’s systems. To this Court, such explicit policies are nothing but “security measures” employers may implement to prevent individuals from doing things in an improper manner on the employer’s computer systems.

Such a view is in accord with the plain language of the statute. Indeed, the *Nosal* panel acknowledged that employer policies restricting the manner of use and access fit the plain language of the CFAA. *See Nosal*, 676 F.3d at 858 (“[T]he CFAA is susceptible to the government’s broad interpretation [.]”). Nevertheless, the *Nosal* panel explicitly rejected this idea, finding that “it is possible to read both prohibitions as applying to hackers.” *Id.*

*15 According to the *Nosal* panel: “ ‘[W]ithout authorization’ would apply to *outside* hackers (individuals who have no authorized access to the computer at all) and ‘exceeds authorized access’ would apply to *inside* hackers (individuals whose initial access to a computer is authorized but who access unauthorized information or files).” *Id.* But this “outside hacker” and “inside hacker” distinction fails to account for the employer’s ability to dictate the manner in which “inside hackers” access unauthorized information or files.

As discussed, the Sixth Circuit in *Pulte Homes* adopted the *Brekka* approach to make clear that an individual only acts “without authorization” when they are *completely* prohibited from accessing, obtaining, or altering anything on a protected computer, *in any manner*. Thus, an employee’s “authorized access” is completely dependent on the scope of the authorization provided by employers,

American Furukawa, Inc. v. Hossain, --- F.Supp.3d ---- (2015)

2015 IER Cases 182,599

who dictate at a threshold level how and what an employee may properly access, obtain, or alter on the employer's computer. As the dissent in *Nosal* explained, "[t]his is not an esoteric concept." *Nosal*, 676 F.3d at 865 (Silverman, J., dissenting). Indeed, the concept was originally advanced by the Ninth Circuit in *Brekka* when they acknowledged that "[t]he plain language of the statute [] dictates that 'authorization' depends on the actions taken by the employer." *Brekka*, 581 F.3d at 1135 (emphasis added).

The Court in *Brekka* explained that, "for purposes of the CFAA, when an employer authorizes an employee to use a company computer subject to certain limitations, the employee *remains authorized to use the computer* even if the employee violates those limitations." *Brekka*, 581 F.3d at 1133 (emphasis added). Because an individual can violate employer-placed limits, yet still have authorization to access an employer's computer; limitations dictating the manner in which the employee may properly access, obtain or alter information on the computer, give full effect to the CFAA's "exceeds authorized access" language.⁶

Foreclosing purpose and use restrictions by employers, simply conflicts with the plain language of the statute. See *Nosal*, 676 F.3d at 864 (Silverman, J., dissenting). If an employee were to take customer information in violation of a use policy to commit widespread identity theft, it would still be the work of an "inside hacker." Cf. *United States v. John*, 597 F.3d 263, 271–73 (5th Cir.2010) (finding an employee of Citigroup exceeded her authorized access in violation of the CFAA when she accessed confidential customer information in violation of her employer's computer use restrictions and used that information to commit fraud).

Moreover, the CFAA provides an avenue to obtain civil relief against this "inside hacker," regardless of whether the employee's actions were part of a criminal scheme. Cf. *United States v. Rodriguez*, 628 F.3d 1258, 1263 (11th Cir.2010) (rejecting the argument that the Defendant should not be liable under the CFAA because his conduct was "not criminal," and noting: "The problem with [the defendant's] argument is that his *use of information is irrelevant if he obtained the information without authorization or as a result of exceeding authorized access.*") (emphasis added).

^{*16} The *Nosal* panel never clearly explains why the CFAA's plain language does not permit computer owners to "spell out explicitly what is forbidden" on its computers. See *EF Cultural Travel B.V. v. Zefer Corp.*, 318 F.3d 58, 63 (1st Cir.2003); see also *United States v. John*, 597 F.3d at 271–73; *United States v. Rodriguez*,

628 F.3d at 1263; *United States v. Salum*, 257 Fed.Appx. at 230; *United States v. Teague*, 646 F.3d at 1121–22. Indeed, that was the interpretation *originally* adopted by the Ninth Circuit. See *Brekka*, 581 F.3d at 1135. Accordingly, this Court finds that the Sixth Circuit would look to the provided definition under the CFAA to find that whether an employee "exceeds authorized access," depends on actions taken by the employer.

ii. There is no need to apply the rule of lenity to interpret the CFAA's "exceeds authorized access" language because Congress provided a clear and unambiguous definition for the phrase.

^[3] The Court's inquiry should end with the unambiguous definition provided by Congress for "exceeds authorized access" because "[i]f the statute is not ambiguous, the use of canons of construction, reference to legislative history, and application of the rule of lenity is not appropriate." *United States v. Lumbard*, No. 1:10–CR–388, 2011 WL 4704890, at *1 (W.D.Mich. Oct. 6, 2011) *aff'd*, 706 F.3d 716 (6th Cir.2013); see also *Dep't of Housing and Urban Dev. v. Rucker*, 535 U.S. 125, 132, 122 S.Ct. 1230, 152 L.Ed.2d 258 (2002); *United States v. Johnson*, 529 U.S. 53, 59, 120 S.Ct. 1114, 146 L.Ed.2d 39 (2000).

Both the Supreme Court of the United States and Sixth Circuit have noted that the rule of lenity only "comes into operation *at the end* of the process of construing what Congress has expressed, not at the beginning as an overriding consideration of being lenient to wrongdoers." *United States v. Adams*, 722 F.3d 788, 804 n. 8 (6th Cir.2013) (quoting *Callanan v. United States*, 364 U.S. 587, 596, 81 S.Ct. 321, 5 L.Ed.2d 312 (1961)) (emphasis added).

The *Nosal* panel never explained how the CFAA's definition for "exceeds authorized access" was ambiguous, yet the panel examined the legislative history of the CFAA to conclude: "If Congress meant to expand the scope of criminal liability to everyone who uses a computer in violation of computer use restrictions ... *we would expect it to use language better suited to that purpose.*" *Nosal*, 676 F.3d at 857 (emphasis added); see also *id.* at 857 n. 3 (citing 18 U.S.C. § 1832(a) to note Congress did, in fact, use specific language "in the federal trade secrets statute [] where it used the common law terms for misappropriation[.]"); *id.* at 858 (stating that the "narrow" construction of "exceeds authorized access is a "perfectly plausible construction of the statutory language" that does not turn the CFAA "into a sweeping

American Furukawa, Inc. v. Hossain, --- F.Supp.3d ---- (2015)

2015 IER Cases 182,599

Internet-policing mandate.”); *id.* at 858 n. 5 (outlining the legislative history to support the “narrow” construction).

*17 However, the judiciary’s “expectation” that Congress would use “better suited” language is not an excuse to encroach upon powers explicitly reserved to the legislative branch. *See Violette v. P.A. Days, Inc.*, 427 F.3d 1015, 1017 (6th Cir.2005) (quoting *Rucker*, 535 U.S. at 134–35, 122 S.Ct. 1230, to note: “To avoid a law’s plain meaning in the absence of ambiguity ‘would trench upon the legislative powers vested in Congress by Art. I, § 1, of the Constitution.’ ”). Unlike the *Nosal* panel, this Court will not read ambiguity into the definition of “exceeds authorized access” at the beginning of its analysis “as an overriding consideration of being lenient to wrongdoers.” *Adams*, 722 F.3d at 804 n. 8 (quoting *Callanan v. United States*, 364 U.S. at 596, 81 S.Ct. 321).

The *Nosal* panel resorted to the CFAA’s legislative history to apply the rule of lenity due to concerns that “millions of unsuspecting individuals would find that they are engaging in criminal conduct.” *Nosal*, 676 F.3d at 859; *see also id.* at 860 (worrying that “[b]asing criminal liability on violations of private computer use policies can transform whole categories of otherwise innocuous behavior into federal crimes simply because a computer is involved [.]” and worrying that a broad reading of the CFAA could turn “minor dalliances” into “federal crimes”).

The *Nosal* panel’s concern was rooted in the fact that “[w]hile it’s unlikely that you’ll be prosecuted for [innocuous conduct] on your work computer, you *could* be.” *Nosal*, 676 F.3d at 860 (emphasis in original); *see id.* at 860 n. 7 (providing a hypothetical of an aggressive prosecutor who might attempt to prosecute an employee who spends six hours a day tending to his FarmVille stable on his work computer in violation of the company’s use policy).⁷

The *Nosal* panel sought to narrow the definition of “exceeds authorized access” in order to “consider how the interpretation [] will operate wherever in [the CFAA] the phrase appears.” *Nosal*, 676 F.3d at 859; *see also id.* (noting that the “phrase appears five times in the first seven subsections of the statute, including subsection 1030(a)(2)(C)”). The panel paid specific attention to Subsection (a)(2)(C), which it labeled as “the broadest” provision because Subsection (a)(2)(C) makes it a crime to access a computer “without any culpable intent.” *Nosal*, 676 F.3d at 859.⁸

Under Subsection (a)(2)(C), the *Nosal* panel found that “the broad interpretation of the CFAA” would allow “private parties to manipulate their computer-use and

personal policies so as to turn these relationships into ones policed by the criminal law.” *Nosal*, 676 F.3d at 860; *see also id.* at 860 n. 6 (noting that “[e]nforcement of the CFAA against minor workplace dalliances is not chimerical,” and stating that a district court case from Florida—where an employer brought claims against an employee under the CFAA—could not have been dismissed if “exceeds authorized access included violations of private computer use policies.”).⁹

*18 Thus, to quell its concerns, the *Nosal* panel rejected the Government’s position that the CFAA’s definition of the phrase “exceeds authorized access” includes use restrictions. *Nosal*, 676 F.3d at 875–58. Instead, to avoid a harsh construction, the *Nosal* panel found that the phrase “exceeds authorized access” only applies to someone who accesses data that the accessor is completely prohibited from obtaining at all, in any manner. *See Nosal*, 676 F.3d at 864.

The Fourth Circuit agreed with the *Nosal* panel, but labeled the Ninth Circuit’s approach the “harsher approach.” *WEC Carolina*, 687 F.3d at 206. The Fourth Circuit found that Congress did not “clearly intend to criminalize” behavior such as “an employee who with commendable intentions disregards his employer’s policy against downloading information to a personal computer so that he can work at home and make headway in meeting his employer’s goal.” *Id.*¹⁰

Despite the unambiguous definition provided by Congress, the *Nosal* panel and the Fourth Circuit resorted to the rule of lenity because they felt Congress *clearly* meant for the CFAA’s “exceeds authorized access” language to be limited to violations of restrictions on access to information. *See Nosal*, 676 F.3d at 863; *WEC Carolina*, 687 F.3d at 206. However, the *Nosal* panel and Fourth Circuit only point out that ridiculous prosecution may occur by including use restrictions; they do not point to any ambiguity in the definition of “exceeds authorized access” provided by Congress.

Given the circumstances, the *Nosal* panel and Fourth Circuit were well-intentioned by seeking to prevent harsh results. However, both the Supreme Court and the Sixth Circuit have cautioned that “[t]he judiciary is not ‘licensed to attempt to soften the clear import of Congress’ chosen words whenever a court believes those words lead to a harsh result.’ ” *Id.* (quoting *United States v. Locke*, 471 U.S. 84, 95, 105 S.Ct. 1785, 85 L.Ed.2d 64 (1985)). All told, “[w]here there is no ambiguity, as is the case here, ‘the rule of lenity does not come into play.’ ” *United States v. Adams*, 722 F.3d at 804 n. 8 (quoting *United States v. Turkette*, 452 U.S. 576, 587 n. 10, 101 S.Ct. 2524, 69 L.Ed.2d 246 (1981)).

American Furukawa, Inc. v. Hossain, --- F.Supp.3d ---- (2015)

2015 IER Cases 182,599

The rule of lenity does not apply here, as both the Supreme Court and Sixth Circuit have cautioned that the rule of lenity “only serves as an aid for resolving an ambiguity; it is not to be used to beget one.” *Adams*, 722 F.3d at 804 n. 8 (6th Cir.2013) (quoting *Callanan v. United States*, 364 U.S. at 596, 81 S.Ct. 321) (emphasis added). The Sixth Circuit found no ambiguity in the CFAA’s definition for “exceeds authorized access,” and searching for or creating possible contrary intent is unwarranted. *P.A. Days, Inc.*, 427 F.3d at 1017 (quoting *Am. Tobacco Co. v. Patterson*, 456 U.S. 63, 75, 102 S.Ct. 1534, 71 L.Ed.2d 748 (1982), to caution that “[g]oing behind the plain language of a statute in search of a possibly contrary congressional intent is a step to be taken cautiously even under the best of circumstances.”). The intent of Congress is clear given the plain language of CFAA’s definition of “exceeds authorized access,” and the Court need not look beyond the definition provided by Congress to determine its intent.

iii. Furukawa properly alleges that Hossain “exceeded authorized access” in order to take files.

*19 ¹⁴ Here, Furukawa has a Removable Media Policy that explicitly requires permission from a manager before accessing files with removable media. See Dkt. No. 1–4. Even under the “narrow” approach advanced by the *Nosal* panel and Fourth Circuit, Hossain would have exceeded authorized access because he removed files in violation of a policy that was focused on how Hossain accessed Furukawa files. This being the case, the Court finds that Furukawa has properly stated a claim under the CFAA that Hossain “exceeded authorized access” by downloading a total of 1,785 files to his external hard drive and two-and-half-years of email from Furukawa’s exchange server files on March 11, 2014 and March 17, 2014.

2. The Michigan Uniform Trade Secrets Act (“MUTSA”) Does Not Preempt Furukawa’s Claims Pursuant To Michigan Law.

¹⁵ Section 8 of the Michigan Uniform Trade Secrets Act (“MUTSA”) preempts claims based on conflicting state tort law and provides civil remedies for misappropriation of trade secrets. See Mich. Comp. Laws § 445.1908(1); *Wysong Corp. v. M.I. Industries*, 412 F.Supp.2d 612, 622–23 (E.D.Mich.2005). However, the MUTSA does not preempt “[o]ther civil remedies that are not based upon

misappropriation of a trade secret.” Mich. Comp. Laws § 445.1908(2).

The critical inquiry for courts in determining whether a claim is displaced by the MUTSA is whether the claim in question is based *solely* on the misappropriation of a trade secret. See *Dura Global Technologies, Inc. v. Magna Donnelly Corp.*, No. 07–10945, 2009 WL 3032594, at *3 (E.D.Mich. Sept. 18, 2009) (quoting *Bliss Clearing Niagara, Inc. v. Midwest Brake Bond Co.*, 270 F.Supp.2d 943 (W.D.Mich.2003)).

¹⁶ If a claim is based solely upon the misappropriation of a trade secret, “the claim must be dismissed.” *Bliss Clearing Niagara, Inc.*, 270 F.Supp.2d at 947; see also *Dura Global Technologies, Inc.*, 2009 WL 3032594, at *3. Conversely, where “a cause of action exists in the commercial area not dependent on trade secrets, that cause continues to exist.” *Id.*; see also *Dura Global Technologies, Inc.*, 2009 WL 3032594, at *3.

Here, Hossain argues that Furukawa’s “Fraud, Breach of Fiduciary Duty, and Conversion claims [] are based on alleged trade secret misappropriation and are preempted [by] Michigan’s Trade Secret Act[.]” Dkt. No. 30 at 14 (citing Mich. Comp. Laws § 445.1908(a)). However, Hossain’s argument fails because Furukawa’s Breach of Fiduciary Duty and Conversion Claims are not “solely based on misappropriation of a trade secret.” *Wysong*, 412 F.Supp.2d at 623.

Furukawa argues it is “also suing for tortious conduct that does not involve misappropriation of information[.]” Dkt. No. 33 at 25. Notably, Hossain actually supports Furukawa’s assertion by acknowledging Furukawa’s claims support causes of action beyond just the misappropriation of trade secrets.¹¹

This being the case, this Court finds that the Complaint alleges facts, independent of the MUTSA claim, supporting causes of action for Fraud, Breach of Fiduciary Duty, and Conversion. See *McKesson Med.-Surgical, Inc. v. Micro Bio-Medics, Inc.*, 266 F.Supp.2d 590, 600 (E.D.Mich.2003) (finding MUTSA did not preempt a claim because the plaintiff’s claim “both according to its Complaint and its Response to Defendants’ Motion, [is] based not only on [the plaintiff’s] trade secrets, but also other confidential information.”); see also *Lube USA Inc. v. Michigan Manufacturers Service Inc.*, 2009 WL 2777332, at *8 (E.D.Mich. Aug. 27, 2009); *Dura Global Technologies, Inc.*, 2009 WL 3032594, at *5.

American Furukawa, Inc. v. Hossain, --- F.Supp.3d ---- (2015)

2015 IER Cases 182,599

3. Furukawa's Employment Handbook Does Not Affect Furukawa's Breach Of Contract Claim.

*20 ^[7] ^[8] In Michigan, if "contract language is clear and unambiguous, its meaning is a question of law." *Gerken Paving Inc. v. LaSalle Grp. Inc.*, No. 10-CV-14905, 2012 WL 3079249, at *4 (E.D.Mich. July 30, 2012) *aff'd*, 558 Fed.Appx. 510 (6th Cir.2014) (quoting *Port Huron Educ. Ass'n v. Port Huron Area Sch. Dist.*, 452 Mich. 309, 550 N.W.2d 228, 237 (1996)).

Hossain argues that Furukawa bases its Breach of Contract claim on documents that are not enforceable contracts by their express terms, because Furukawa's "Policies and Practices Handbook" explicitly notes that "the adoption of this employee handbook is entirely voluntary on the part of the company and shall not be construed as creating a contractual relationship between the company and any employee. It is neither a contract nor an agreement of employment for a definite period of time[.]" Dkt. No. 30 at 17 n. 3 (quoting Dkt. No. 1-3 at 26).

However, the Court need not address the Policies and Practice Handbook with respect to the Breach of Contract claim because Furukawa's Breach of Contract Claim is only premised on the "Invention Assignment & Secrecy Agreement," *see* Dkt. No. 1 at ¶ 120, and, impliedly, Furukawa's Removable Media Policy. *See id.* at ¶ 122. Hossain argues that Furukawa's Removable Use Policy is only a "guide," but the Court sees nothing in the Removable Media Use Policy indicating it is meant to be a guide by its express terms. *See* Dkt. No. 1-4 at 2. Moreover, Hossain does not even address the Invention Assignment & Secrecy Agreement as it pertains to the Breach of Contract claim. *See* Dkt. No. 40 at 18 (arguing that the Breach of Contract claim should be dismissed "to the extent it relies upon exhibits 1, 2, and 3[.]"). Thus, the Court finds nothing in the Removable Media Policy nor the Invention Assignment & Secrecy Agreement that warrants the dismissal of Furukawa's Breach of Contract claim.

4. Furukawa's Conversion Claim Is Properly Alleged Where Hossain Allegedly Took Emails From Furukawa's Servers.

^[9] ^[10] In Michigan, conversion arises from "any distinct act of domain wrongfully exerted over another's personal property in denial of or inconsistent with the rights therein." *Llewellyn-Jones v. Metro Prop. Grp., LLC*, 22 F.Supp.3d 760 (E.D.Mich.2014) (citing *Foremost Ins. Co. v. Allstate Ins. Co.*, 439 Mich. 378, 391, 486 N.W.2d 600 (1992)); *see also Murray Hill Publ'ns, Inc. v. ABC Comme'ns, Inc.*, 264 F.3d 622, 636-37 (6th Cir.2001).

Hossain argues that Furukawa's conversion claim should be dismissed because Furukawa "attached various email communications from companies and individuals who are distinct and unrelated" to Furukawa to support the claim for Conversion. *See* Dkt. No. 30 at 18. The Court disagrees. The Court points out that *all* of the documents and information allegedly removed were removed from Furukawa's servers. As Furukawa points out, "[t]he fact that some of the information 'pertains to third parties unrelated to Plaintiff,' does not negate the information as being personal property belonging to [Furukawa]; nor has [Hossain] cited any authority for that proposition." Dkt. No. 33 at 28.

*21 Indeed, "Michigan appellate courts have held that certain intangible property can be the subject of a conversion action." *Sarver v. Detroit Edison Co.*, 225 Mich.App. 580, 586, 571 N.W.2d 759, 762 (1997) (citations omitted). In each case where the Michigan courts have found that the intangible property can be the subject of a conversion action, "the plaintiff's ownership interest in intangible property was represented by or connected with something tangible." *Id.*

Here, even though *some* emails on the server contain information pertaining to third parties, the emails were still sent to Furukawa, stored inside Furukawa's tangible property, and constituted trade secrets. *See Wysong*, 412 F.Supp.2d at 630 ("the plaintiff's supplier contact data meets the definition of a protectable trade secret"); *id.* at 629 ("customer lists developed by a former employee and information relating to a customer's needs are not "trade secrets" under the MUTSA, *unless the employee is bound by a confidentiality agreement.*") (emphasis added). Accordingly, looking at the Complaint in a light most favorable to Furukawa, Furukawa has set forth a proper claim for conversion since Hossain took 1,785 files and two-and-half-years of email from Furukawa's exchange server and placed the information on his external hard drive.

VI. CONCLUSION

For the reasons discussed, the Court **DENIES** Defendant Hossain's Motion for Partial Judgment on the Pleadings [30].

SO ORDERED.

American Furukawa, Inc. v. Hossain, --- F.Supp.3d ---- (2015)

2015 IER Cases 182,599

All Citations

--- F.Supp.3d ----, 2015 WL 2124794, 2015 IER Cases 182,599

Footnotes

- 1 A “protected computer” is defined as any computer “used in or affecting interstate or foreign commerce or communication[.]” 18 U.S.C. § 1030(e)(2)(B).
- 2 The CFAA defines the term “damage” as “any impairment to the integrity or availability of data, a program, a system, or information [.]” 18 U.S.C. § 1030(e)(8).
- 3 The CFAA indicates that “the term ‘loss’ means any reasonable cost to any victim[.]” 18 U.S.C. § 1030(11). Specifically, the CFAA explains that loss includes “the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service[.]” *Id.*
- 4 A helpful analogy for the application of the “narrow” interpretation of the CFAA’s “without authorization” language was explained in a district court opinion out of the Eastern District of Pennsylvania:
 An analogy to burglary provides clarity ... “If a person is invited into someone’s home and steals jewelry while inside, the person has committed a crime—but not burglary—because he has not broken into the home. The fact that the person committed a crime while inside the home does not change the fact that he was given permission to enter.”
Dresser–Rand Co. v. Jones, 957 F.Supp.2d 610, 614 (E.D.Pa.2013) (quoting Thomas E. Booms, *Hacking into Federal Court: Employee “Authorization” Under the Computer Fraud and Abuse Act*, 13 VAND. J. ENT. & TECH. L.. 543, 571 (2011)).
- 5 The Court is aware that Hossain was still employed by Furukawa while on his leave of absence, this does not overshadow the fact that Furukawa took overt steps to revoke Hossain’s access such that he would recognize he was “without authorization.” *See, e.g., Steele*, 595 Fed.Appx. at 211 (noting the defendant in that case “clearly acted ‘without authorization’ under the plain meaning of the CFAA” because: “Common sense aside, the evidence provides ample support for the jury’s verdict. [The company] took steps to revoke [the defendant’s] access to company information, including collecting [the defendant’s] company-issued laptop, denying him physical access to the company’s offices, and generally terminating his main system access. And [the defendant] himself recognized that his resignation effectively terminated any authority he had to access [the company’s] server, promising in his resignation letter that he would not attempt to access the system thereafter. Just because [the company] neglected to change a password on [the defendant’s] backdoor account does not mean [the company] intended for [the defendant] to have continued access to its information.”).
- 6 For example, a company may explicitly instruct a driver that he/she can only access the company’s car to deliver the company’s pizzas; provided the driver delivers the pizzas *in the manner* the company dictates he/she can use the company’s car. The driver’s access to the car—the driver’s entitlement/authorization—will remain so long as the driver does not go beyond the instructions provided by the company regarding the use of the car. However, the driver would not be entitled/authorized—the driver would “exceed authorized access”—to use the company’s car to deliver a competing company’s pizza; sell drugs out of the company’s car; or do anything else beyond of the scope of *how* the driver was instructed to use the company’s car.
- 7 However, this concern does not warrant avoiding a definition provided by Congress. The Court agrees prosecuting an individual for using his FarmVille account at his job “does not appear to be a worthy way to expend valuable law enforcement resources.” *Lawrence v. Texas*, 539 U.S. 558, 605, 123 S.Ct. 2472, 156 L.Ed.2d 508 (2003) (Thomas, J., dissenting). Nevertheless, just because inane prosecutions are possible, it does not mean that the statutes underlying the prosecutions are flawed.
- 8 However, this concern is overstated because liability under the CFAA will not attach unless an individual accesses a computer *and* obtains something to which they are not entitled. So even if an individual exceeds authorized access by accessing Facebook in a wrongful manner, in order for liability to attach the individual would *still* have to obtain something to which they were not entitled so to obtain or alter. *See, e.g., Lee v. PMSI, Inc.*, No. 8:10–CV–2904–T–23TBM, 2011 WL 1742028, at *2 (M.D.Fla. May 6, 2011) (“Because the only information [the employee] allegedly accessed was on [] personal websites, not [the employer’s] computer system, [the employee] never ‘obtained or alter[ed] information in the computer.’ [The employee] accessed her facebook, personal email, and news websites but did not access any information that she was ‘not entitled so to obtain or alter.’ ”).
- 9 However, the Florida case *could* have been dismissed if “exceeds authorized access included violations of private computer use policies.” It is important to note that *Lee v. PMSI, Inc.* was a civil action. No. 8:10–CV–2904–T–23TBM, 2011 WL 1742028 (M.D.Fla. May 6, 2011). The *Nosal* panel does not account for the fact that, in order to be civilly liable that under CFAA, there must be damage or loss to one or more persons during any one-year period aggregating to at least \$5,000 in value. *See* 18 U.S.C. §

American Furukawa, Inc. v. Hossain, --- F.Supp.3d ---- (2015)

2015 IER Cases 182,599

1030(c)(4)(A)(i)(I). Indeed, the counterclaim by the employer in *PMSI, Inc.* was dismissed, in part, because the employer could not show there was sufficient damage or loss caused by the employee simply accessing Facebook at work. *See PMSI, Inc.*, 2011 WL 1742028, at *1 (“The [CFAA] does not contemplate ‘lost productivity’ of an employee, and with the exception of the loss of productivity, the defendant fails to allege ‘damage’ caused by the plaintiff’s internet usage.”).

10 Again, however, this concern does not warrant avoiding a definition provided by Congress. The Court agrees that such a prosecution by a federal prosecutor would be silly. Nevertheless, this Court must decide this case based on CFAA as Congress unambiguously wrote it; “[i]t is the essence of judicial duty to subordinate [this Court’s] own personal views, [and] ideas of what legislation is wise and what is not.” *Griswold v. Connecticut*, 381 U.S. 479, 530–31, 85 S.Ct. 1678, 14 L.Ed.2d 510 (1965) (Stewart, J. dissenting).

11 *See, e.g.*, Dkt. No. 30 at 15 (Hossain citing Dkt. No. 1 at ¶ 115 to note: “Plaintiff’s fraud claim alleges that Plaintiff relied on Mr. Hossain’s representations by allowing him to have access to trade secret and confidential and proprietary information *which led to unfair competition*”) (emphasis added); *id.* (Hossain citing Dkt. No. 1 at ¶ 128 to note: “Plaintiff’s breach of fiduciary duty claim, alleges that Mr. Hossain violated a purported duty of good faith and loyalty by using Plaintiff’s trade secrets *and other information to divert business away from Plaintiff and assist[] Huatong to compete against Plaintiff.*”) (emphasis added); *id.* at 16 (Hossain citing Dkt. No. 1 at ¶¶ 144–45 to note: “Plaintiff’s conversion claim alleges Mr. Hossain had access to Plaintiff’s trade secret *and other confidential information*”). (emphasis added).

End of Document

© 2015 Thomson Reuters. No claim to original U.S. Government Works.

Bailey v. Bailey, Not Reported in F.Supp.2d (2008)

2008 WL 324156

Only the Westlaw citation is currently available.

United States District Court,
E.D. Michigan,
Southern Division.

Deborah Jo BAILEY, Plaintiff,
v.
Jeffery Allan BAILEY, et al., Defendants.

No. 07-11672. | Feb. 6, 2008.

Attorneys and Law Firms

C. Bruce Lawrence, Lapeer, MI, for Plaintiff.

Donald G. Rockwell, Nill Rockwell, Flint, MI, Theresa M. Asoklis, Collins, Einhorn, Southfield, MI, for Defendants.

Andrew J Kozyra, Dryden, MI, pro se.

OPINION AND ORDER

SEAN F. COX, District Judge.

*1 This matter is before the Court on Defendant Jeffrey Bailey's Motion for summary judgment; and Defendant Todd Pope's Motion for summary judgment. All parties have briefed the issues and a hearing was held January 17, 2008. For the following reasons, the Court **GRANTS** Defendant Todd Pope's Motion for summary judgment; and **GRANTS** in part, and **DENIES** in part, Defendant Jeffrey Bailey's Motion for summary judgment. Summary judgment is granted on Plaintiff's claims for: (1) violation of 18 U.S.C. § 2511; (2) violation of 18 U.S.C. § 2512; (3) MCL § 750.539a, et seq.; (4) MCL § 750.540; (5) invasion of privacy against Defendant Pope based on intrusion upon seclusion; (6) invasion of privacy based on public disclosure; and (7) intentional infliction of emotional distress. Summary judgment is denied on Plaintiff's claims for: (1) violation of 18 U.S.C. § 2701 against Defendant Bailey; and (2) invasion of privacy against Defendant Bailey based on intrusion upon seclusion. Additionally, Defendant Andrew Kozyra is **DISMISSED** from this action.

I. BACKGROUND

This case arises out of Defendant Jeffrey Bailey's installation of a key logger on a computer shared by him and his now ex-wife, Plaintiff Deborah Jo Bailey.

Plaintiff and Defendant Bailey were married in 1987 and had three children. Unfortunately, the marriage began to deteriorate. Defendant Bailey had suspicions about Plaintiff's use of the internet, which he believed was excessive. According to Defendant Bailey, in fall of 2005 he clicked onto his wife's email account, titled *joy2u*. He saw several alerts that there were messages for Plaintiff from a website called Killer Movies Forum. Defendant Bailey clicked on the hyperlink associated with the alerts and read the messages. The messages were from a person known as "Finti" and were of a sexual nature. Plaintiff admitted to sexual discussions with Finti and others, but denies her children were aware of the discussions.

Shortly after Defendant Bailey discovered Plaintiff's sexual discussions, she opened a new email account titled *chloedebb@yahoo.com*. Around the same time, Defendant Bailey downloaded a free trial version of a key logger software and installed it on both home computers. The program is designed to record every keystroke made on the computer and store it in a text file on the computer's hard drive. The parties dispute whether the file storing the keystroke information can be accessed only on the computer where the software is installed, or whether it can be accessed remotely. Defendant Bailey used the key logger program to learn the password for both Plaintiff's *chloedebb@yahoo.com* email account and her private messaging system on the Killer Movies Forum. Defendant Bailey learned that Plaintiff was continuing her internet sexual activities.

On January 9, 2006, Defendant Bailey left the marital home with the three children and went to Ohio to stay with his brother. In anticipation of divorce proceedings, Defendant Bailey provided his attorney, Defendant Todd Pope, with copies of emails and messages taken from the home computer. Throughout the divorce proceedings, Defendant Bailey supplied Defendant Pope with copies of emails and messages he said he was able to access because he had Plaintiff's passwords, by virtue of the key logger program. However, Defendant Bailey denies that he accessed the key logger program on the home computer after he left on January 9, 2006. Instead, he claims he continued to access Plaintiff's accounts using the passwords he had obtained using the key logger, or by guessing her new passwords which he claims all used

Bailey v. Bailey, Not Reported in F.Supp.2d (2008)

family names. Plaintiff also had her daughter Chloe set up another email account titled debbiejo_crazy@yahoo.com. Chloe gave the password to Defendant Bailey.

*2 Defendant Bailey filed for divorce on January 11, 2006. He alleged Plaintiff was an alcoholic with a history of depression and sought full physical custody of the children.

Defendant Bailey was granted temporary custody. Plaintiff hired an attorney, Defendant Andrew Kozyra. The custody order was amended to grant Plaintiff parenting time every third weekend, with the condition that neither party was allowed to consume alcohol during their parenting time. During further custody proceedings, Plaintiff testified that she had not consumed alcohol recently and was voluntarily undergoing alcohol and drug testing. Defendant Pope impeached her testimony using emails provided to him by Defendant Bailey. The emails indicated that Plaintiff had recently gone to a party where she consumed alcohol and illegal drugs.

On May 18, 2006, Defendant Pope sent a request to admit the genuineness of the email and message copies provided by Defendant Bailey, to Defendant Kozyra. Defendant Kozyra, on behalf of Plaintiff, moved for a protective order. His request was denied.

On July 16, 2006, Plaintiff was cited for a second drinking offense. The parties settled the divorce case prior to the July 21, 2006 trial date. Plaintiff agreed to give full physical custody of the children to Defendant Bailey. Plaintiff was to receive parenting time, including two nonconsecutive weeks in the summer. The judgment of divorce was entered on August 31, 2006. Within two weeks of entry of the judgment, Plaintiff was again arrested for driving while intoxicated. Defendant Bailey moved to suspend Plaintiff's parenting time. At the hearing, the judge indicated he was very concerned about Plaintiff's sobriety. A hearing was held on January 5, 2007 on Defendant Bailey's motion to suspend parenting time. At the hearing, the judge heard testimony that Plaintiff made allegations of sexual assault against Defendant Bailey regarding their daughter Chloe. He also heard testimony from a neighbor that during a visit in August, Plaintiff was "highly intoxicated" and the neighbor took care of the children while Defendant Bailey drove from Ohio to pick them up. The parties' daughter Chloe also testified that she had witnessed her mother intoxicated during the visit. The judge concluded Plaintiff was harming her children and suspended her parenting time. After this hearing, Plaintiff was arrested for domestic violence against Defendant Bailey and found in contempt of court for emailing her children. At a March 2, 2007 hearing, the judge awarded sole legal and physical

custody to Defendant Bailey. Plaintiff has only recently been given parenting time in the form of supervised visitation one weekend per month at her father's home.

Plaintiff argues that she would not have lost custody of her children if her emails and internet messages had not been disclosed. She also attributes emotional problems and distress she claims to suffer to the loss of custody of her children.

*3 On April 13, 2007, Plaintiff filed the instant action. On August 28, 2007, an Amended Complaint was filed alleging: (1) violation of 18 U.S.C. § 2511 against Defendants Bailey and Pope; (2) violation of 18 U.S.C. § 2701 against Defendant Bailey; (3) violation of 18 U.S.C. § 2512 against Defendants Bailey and Pope, and against a John Doe Defendant who supplied the key logger software; (4) violations of MCL § 750.539a, et seq., and MCL § 750.540 against Defendants Bailey, Pope and John Doe; (5) invasion of privacy against Defendants Bailey and Pope; (6) intentional infliction of emotional distress against all Defendants; and (7) professional malpractice against Defendant Kozyra. Also on April 13, 2007, Plaintiff filed a motion for preliminary injunction to prevent further use of the key logger software, the parties entered a stipulation following a status conference.

On October 22, 2007, Defendants Bailey and Pope filed separate Motions for summary judgment as to all claims.

II. STANDARD OF REVIEW

Under Fed. R. Civ. P. 56(c), summary judgment may be granted "if the pleadings, depositions, answers to interrogatories, and admissions on file, together with the affidavits, if any, show that there is no genuine issue as to any material fact and that the moving party is entitled to judgment as a matter of law." *Copeland v. Machulis*, 57 F.3d 476, 478 (6th Cir.1995). A fact is "material" and precludes a grant of summary judgment if "proof of that fact would have [the] effect of establishing or refuting one of the essential elements of the cause of action or defense asserted by the parties, and would necessarily affect application of appropriate principle[s] of law to the rights and obligations of the parties." *Kendall v. Hoover Co.*, 751 F.2d 171, 174 (6th Cir.1984). The court must view the evidence in the light most favorable to the nonmoving party and it must also draw all reasonable inferences in the nonmoving party's favor. *Cox v. Kentucky Dept. of Transp.*, 53 F.3d 146, 150 (6th Cir.1995).

III. ANALYSIS

A. 18 U.S.C. § 2511-The Wiretap Act

Plaintiff alleges Defendants Pope and Bailey violated 18 U.S.C. § 2511 when they obtained Plaintiff's emails and messages using the passwords learned from the key logger. Section 2511 provides, in pertinent part:

(1) Except as otherwise specifically provided in this chapter any person who-

(a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;

* * *

(c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;

(d) intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection ...

*4 shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).

The parties dispute whether Defendants' conduct is actionable under the Wiretap Act because, according to Defendants, there was no "interception" as that term has been interpreted by the courts. Specifically, the parties disagree on whether "interception" requires that the electronic communication be intercepted contemporaneously with its transmission. There is no Sixth Circuit authority on the issue.

Although the issue has not been addressed by the Sixth Circuit, the Circuits that have addressed the issue have agreed that the definition of "intercept" "encompasses only acquisitions contemporaneous with transmission." *United States v. Steiger*, 318 F.3d 1039, 1047 (11th Cir.2003). See *Steve Jackson Games, Inc. v. United States Secret Service*, 36 F.3d 457 (5th Cir.1994); *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868 (9th Cir.2001); *In re Pharmatrac, Inc.*, 329 F.3d 9 (1st Cir.2003); and *Fraser v. Nationwide Mutual Ins. Co.*, 352 F.3d 107 (3rd Cir.2003). The general reasoning behind these decisions

is that based on the statutory definition and distinction between "wire communication" and "electronic communication," the latter of which conspicuously does not include electronic storage, Congress intended for electronic communication in storage to be handled solely by the Stored Communications Act. This interpretation is reasonable and consistent with the language of the statute.

Plaintiff does not offer argument or authority that contradicts the reasoning offered by the cases cited above. Instead, Plaintiff directs this Court to the "leading case" of *United States v. Councilman*, 418 F.3d 67 (1st Cir.2005). Plaintiff claims that the *Councilman* court "determined that the contemporaneous requirement which had been inserted by earlier courts, was not a requirement under a proper interpretation of the Electronic Communications Privacy Act ..." [Response, p. 4]. Plaintiff mischaracterizes the *Councilman* case. First, the *Councilman* court did not address the issue of whether the contemporaneous requirement applied: "this appeal does not implicate the question of whether the term 'intercept' applies only to acquisitions that occur contemporaneously with the transmission of a message from sender to recipient ..." *Id.* at 80. What the *Councilman* court ruled was that the term "electronic communication" as used in the Wiretap Act includes "the transient electronic storage that is intrinsic to the communication process for such communications." *Id.* at 79. In *Councilman*, the defendant argued that because the original transmission of an email over the internet involves several minuscule stops at other computers, the Wiretap Act did not apply because it did not encompass electronic communications that were in electronic storage no matter how brief the storage. The *Councilman* court, after an exhaustive analysis, did not agree.

*5 This case is more analogous to *Steiger*, *supra*. In *Steiger*, an anonymous source hacked into the defendant's computer by using a "Trojan Horse" virus. Once the virus was downloaded, the anonymous source was able to access and download information stored on the defendant's computer. The anonymous source found evidence of child sexual abuse and turned the defendant over to the proper authorities. The virus used in *Steiger* only allowed the source to access the defendant's files, it did not "intercept" them while in transit. Similar to the *Steiger* case, here, the key logger only allowed Defendant Bailey to learn passwords, which were used to access and copy Plaintiff's email and messages. Defendant Bailey did not obtain the emails or messages contemporaneously with their transmission, and thus, the Wiretap Act does not apply.

Defendants are entitled to summary judgment on Plaintiff's claim for violation of 18 U.S.C. § 2511.

Bailey v. Bailey, Not Reported in F.Supp.2d (2008)

B. 18 U.S.C. § 2701-Stored Communications Act

Plaintiff alleges Defendant Bailey violated 18 U.S.C. § 2701 when he accessed her emails and messages. Section 2701 provides, in pertinent part:

(a) **Offense**—Except as provided in subsection (c) of this section whoever—

(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or

(2) intentionally exceeds an authorization to access that facility;

and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.

“Electronic storage is defined as either “(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication.” 18 U.S.C. § 2510(17).

Defendant Bailey argues that the Stored Communications Act does not apply because the emails and messages he accessed were already opened by Plaintiff. Defendant Bailey conflates the two meanings of “electronic storage” and states that “electronic storage” “renders only those stored communications which are temporarily stored or stored for purposes of backup protection incidental to the electronic transmission thereof.” [Motion, p. 18]. From this Defendant Bailey concludes that once the electronic communication is transmitted to its intended recipient, the Stored Communications Act no longer applies. Defendant Bailey does not cite any significant authority to support his interpretation. He directs the Court to *Bansal v. Russ*, 513 F.Supp.2d 264, 276 (E.D.Pa.2007), where the Pennsylvania district court, without providing any analysis or citation to authority, found that “[t]he Stored Communications Act ... does not prohibit ... obtaining ‘opened’ emails.” Defendant Bailey also relies on *Fraser*, 352 F.3d 107, for the proposition that emails that were accessed were not in temporary storage, or backup storage, but were in post transmission storage. However, what the *Fraser* court actually held was:

*6 Rather, according to the District Court, the e-mail was in a state it described as ‘post-transmission storage.’ We agree that Fraser’s e-mail was not in temporary, intermediate storage. But to us it seems questionable that the transmissions were not in backup storage—a term that neither the statute nor the legislative history defines. Therefore, while we affirm the District Court, we do so through a different analytical path, assuming without deciding that the e-mail in question was in backup storage.

Id. at 114. Thus, the Fraser case is of no value on this issue.

The Sixth Circuit has not ruled on this issue. However, Defendant’s argument was considered by the Ninth Circuit in *Theofel v. Farey-Jones*, 359 F.3d 1066 (9th Cir.2003). *Theofel* stems from commercial litigation. The defendant sought access to the plaintiff’s email and served an obviously over broad subpoena on the plaintiff’s internet service provider (“ISP”). Due to the large number of documents encompassed by the subpoena, the ISP provided a sample containing 339 emails. Included in the sample were emails that did not pertain to the matter at hand, and that contained personal or privileged information. Several of the individuals affected brought suit against the defendant alleging violation of the Stored Communications Act. The district court dismissed the plaintiffs’ case finding that the access was authorized due to the subpoena. The circuit court disagreed, because the scope of the subpoena was so overly broad the defendant’s knew they were not entitled to access all of the documents requested. Similar to Defendant Bailey’s argument, the defendant made the alternative argument that emails remaining on the ISP’s server after delivery do not fall within the Stored Communications Act’s coverage. The court disagreed. The court held that those messages were not within the purview of the subsection (A) definition, but fit comfortably in subsection (B). The court stated:

There is no dispute that messages remaining on NetGate’s server after delivery are stored ‘by an electronic communication service’ within the meaning of 18 U.S.C. § 2510(17)(B). The only issue, then, is whether the messages are stored ‘for purposes of backup protection.’ 18 U.S.C. § 2510(17)(B). We think that, within the ordinary meaning of those terms, they are.

Bailey v. Bailey, Not Reported in F.Supp.2d (2008)

An obvious purpose for storing a message on an ISP's server after delivery is to provide a second copy of the message in the event that the user needs to download it again-if, for example, the message is accidentally erased from the user's own computer. The ISP copy of the message functions as a 'backup' for the user. Notably, nothing in the Act requires that the backup protection be for the benefit of the ISP rather than the user. Storage under these circumstances thus literally falls within the statutory definition.

Theofel, 359 F.3d at 1075 (internal citations omitted).

This court agrees with the reasoning in *Theofel*. The fact that Plaintiff may have already read the emails and messages copied by Defendant does not take them out of the purview of the Stored Communications Act. The plain language of the statute seems to include emails received by the intended recipient where they remain stored by an electronic communication service. The phrase "such communication" in § 2510(17)(B) refers to "wire or electronic communications" as mentioned in (17)(A)-it does not also include the requirement that the electronic communications be "incidental to the electronic transmission thereof." If that were the case, there would be no need to write them as two separate meanings. However, as a point of clarification, Stored Communications Act protection does not extend to emails and messages stored only on Plaintiff's personal computer. *In re Doubleclick Inc.*, 154 F.Supp.2d 497, 511 (S.D.N.Y.2001) ("the cookies' residence on plaintiffs' computers does not fall into § 2510(17)(B) because plaintiffs are not 'electronic communication service' providers."). Defendant does not set forth any other basis for dismissing the claim. Accordingly, Defendant Bailey is not entitled to summary judgment on Plaintiff's claim for violation of 18 U.S.C. § 2701.

C. 18 U.S.C. § 2512-Wiretap Act

*7 Plaintiff alleges violation of 18 U.S.C. § 2512 against Defendants Bailey, Pope and a John Doe, the manufacturer of the key logger software. However, there is no private right of action under § 2512. 18 U.S.C. § 2520 provides:

(a) In general.-Except as provided in section 2511(2)(a)(ii), any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter may in a civil action recover from the person or entity,

other than the United States, which engaged in that violation such relief as may be appropriate.

Based on the clear language of the statute, a civil cause of action arises only when violation of the statute results in a person's wire, oral, or electronic communication being intercepted, disclosed, or intentionally used. Here, Plaintiffs allegation of violation of § 2512 does not satisfy the requirements of § 2520. Section 2512 deals with the manufacture, sale and possession of particular devices. Violation of the statute has nothing to do with the actual interception, disclosure or use of Plaintiff's electronic communication. See *DIRECTV, Inc. v. Treworgy*, 373 F.3d 1124 (11th Cir.2004).

Accordingly, Defendants are entitled to summary judgment on Plaintiff's claim for violation of 18 U.S.C. § 2512.

D. MCL § 750.539a, et seq.-Eavesdropping Statutes

Plaintiff alleges various violations of Michigan's eavesdropping statutes against Defendants Bailey and Pope.

Defendant Bailey argues the Michigan statutes do not apply because the key logger software is not a "device" as contemplated by the eavesdropping statutes. Defendant Pope argues the Michigan eavesdropping statutes do not apply because Defendant Bailey did not "eavesdrop" on a "private conversation." Plaintiff, without citation to authority, states that the federal Wiretap Act definition of device is analogous to the definition intended by the Michigan eavesdropping statutes, and thus the key logger is a device. Plaintiff does not respond to Defendant Pope's arguments.

A plain reading of the eavesdropping statutes indicates that they do not apply to the circumstances of this case. MCL § 750.539c provides:

Any person who is present or who is not present during a private conversation and who wilfully uses any device to eavesdrop upon the conversation without the consent of all parties thereto, or who knowingly aids, employs or procures another person to do the same in violation of this section, is guilty of a felony punishable by imprisonment in a state prison for

Bailey v. Bailey, Not Reported in F.Supp.2d (2008)

not more than 2 years or by a fine of not more than \$2,000.00, or both.

MCL § 750.539d provides, in pertinent part:

(1) Except as otherwise provided in this section, a person shall not do either of the following:

(a) Install, place, or use in any private place, without the consent of the person or persons entitled to privacy in that place, any device for observing, recording, transmitting, photographing, or eavesdropping upon the sounds or events in that place.

*8 (b) Distribute, disseminate, or transmit for access by any other person a recording, photograph, or visual image the person knows or has reason to know was obtained in violation of this section.

* * *

With respect to § 750.539c, the device must be used with respect to a "conversation." The key logger software only stores as a text file the keys that are pressed on the keyboard of the computer on which the software is installed. When Plaintiff pressed the keys to enter her passwords, compose messages, or compose emails, she was not engaging in a conversation. First, she was not in a direct dialogue with anyone else. Second, the device, the key logger, only recorded her keystrokes, not the response of the other side. The Merriam-Webster Dictionary defines "conversation" as "(1) oral exchange of sentiments, observations, opinions, or ideas; (2) an instance of such exchange." MERRIAM-WEBSTER ONLINE DICTIONARY. The "device" does not record an exchange, but only records keystrokes. This statute was meant to prohibit eavesdropping in the traditional sense of recording or secretly listening to audible conversation. This is bolstered by the fact that the Michigan legislature felt the need to add a statute that deals specifically with the reading or copying of any message from a computer without authorization. MCL § 750.540. Section 750.540 would be redundant if § 750.539c already prohibited the same. Accordingly, Defendants are entitled to summary judgment on Plaintiff's claim of violation of MCL § 750.539c.

With respect to MCL § 750.539d, the device must observe, record, transmit, photograph, or eavesdrop "upon the sounds or events in that place." This description does not encompass a key logger which only records electronically what keystrokes are pressed on a keyboard. It does not record sounds or events. Further, as discussed

above, if that were the contemplated scope of § 750.539d, there would have been no need for § 750.540. Defendants are entitled to summary judgment on Plaintiff's claim for violation of MCL § 750.539d.

Plaintiff also alleges violations for MCL §§ 750.539e and 750.539j. Defendants are entitled to summary judgment on Plaintiff's claim for violation of § 750.539e because it is dependent on the use of information obtained in violation of the eavesdropping statutes, which Defendants are found not to have violated. Defendants are entitled to summary judgment on Plaintiff's claim for violation of § 750.539j because a civil action does not arise from violation of that statute. MCL § 750.539h provides that civil remedies are available only to parties to a conversation upon which eavesdropping is practiced, which is not the substance of a § 750.539j violation.

E. MCL § 750.540

Plaintiff alleges a violation of MCL § 750.540 against Defendants Bailey and Pope. Section 750.540 prohibits the reading or copying of messages sent via a computer without authorization. However, violation of MCL § 750.540 does not appear to give rise to civil liability. The language of § 750.540 only addresses criminal sanctions, it does not mention civil penalties. Moreover, the only statute in the chapter that discusses civil liability is MCL § 750.539h, which states "[a]ny parties to any conversation upon which eavesdropping is practiced contrary to this act shall be entitled to the following civil remedies." As discussed above, Plaintiff's allegations do not amount to eavesdropping of a conversation as contemplated by the eavesdropping statutes. Thus, § 750.539h does not serve to supply a civil cause of action for violation of § 750.540.

*9 "The general rule of law in Michigan is that, where a new right is created or a new duty is imposed by a statute, the remedy provided by the statute for enforcement of the right or for nonperformance of the duty is exclusive unless the remedy is plainly inadequate." *Forster v. Delton School District*, 176 Mich.App. 582, 584, 440 N.W.2d 421 (Mich.App.1989). "Therefore a private cause of action must be dismissed under a statute creating a new right or imposing a new duty unless the private cause of action was expressly created by the act or inferred from the fact that the act provides no adequate means of enforcement of its provisions." *Id.* at 585, 440 N.W.2d 421. Here, § 750.540 does not expressly provide for a private cause of action, and does provide for adequate enforcement by creating criminal penalties. See *Central Bank of Denver v. First Interstate Bank of Denver*, 511 U.S. 164, 190, 114 S.Ct. 1439, 128 L.Ed.2d 119 (1994)

Bailey v. Bailey, Not Reported in F.Supp.2d (2008)

("[W]e refuse[] to infer a private right of action from 'a bare criminal statute'... [a]nd we have not suggested that a private right of action exists for all injuries caused by violations of criminal prohibitions."). Accordingly, Defendants are entitled to summary judgment on Plaintiff's claim for violation of § 750.540.

F. Invasion of Privacy

Plaintiff alleges a claim for invasion of privacy against Defendants Bailey and Pope. The tort of invasion of privacy has four distinct theories, in this case, Plaintiff alleges two theories: (1) the intrusion upon another's seclusion; and (2) a public disclosure of private facts about the individual. *Lewis v. LeGrow*, 258 Mich.App. 175, 193, 670 N.W.2d 675 (Mich.App.2003).

1. Intrusion upon seclusion

"There are three necessary elements to establish a prima facie case of intrusion upon seclusion: (1) the existence of a secret and private subject matter; (2) a right possessed by the plaintiff to keep that subject matter private; and (3) the obtaining of information about that subject matter through some method objectionable to a reasonable man." *Id.* "An action for intrusion upon seclusion focuses on the manner in which the information was obtained, not on the information's publication." *Id.*

As an initial matter, this cause of action cannot be maintained against Defendant Pope because there is no evidence that he participated in the "intrusion." The fact that Pope was aware of how Defendant Bailey obtained the emails and messages is irrelevant. See *Doe v. Mills*, 212 Mich.App. 73, 89-91, 536 N.W.2d 824 (Mich.App.1995). Defendant Pope is entitled to summary judgment on this claim.

With respect to Defendant Bailey, he argues that Plaintiff cannot establish a claim because his actions are not objectionable to a reasonable man. Defendant Bailey contends that his actions were done after inadvertently discovering his wife was having sexual discussions on the internet, and were done to protect himself and his family. Plaintiff responds by stating there is a question of fact, but does not identify any authority or evidence to support his conclusion.

*10 The facts are largely undisputed in this case. The method used by Defendant Bailey was a key logger that recorded Plaintiff's keystrokes, which Defendant used to learn Plaintiff's passwords. With the passwords, Defendant was able to access Plaintiff's email and private

message forums. In addition, once Defendant learned that Plaintiff used family names as passwords, he claims he was able to guess her new passwords even after she repeatedly changed them. Plaintiff avers that Defendant continued to access her email even after divorce proceedings were complete. [Plaintiff's Exhibit A]. She provides an affidavit that claims she planted a false story of an affair with a neighbor in an email on January 2007, well after the divorce was final. She claims that on February 16, 2007, her daughter Chloe sent an email referencing the planted story, which Plaintiff takes to mean Defendant Bailey was continuing to access her accounts and passing the information to their teenage daughter.

Defendant cites *Lewis v. Dayton-Hudson*, 128 Mich.App. 165, 339 N.W.2d 857 (Mich.App.1983), to support his contention that he is entitled to summary judgment. Defendant appears to rely on *Lewis* for the proposition that Plaintiff did not have a right of privacy. In *Lewis*, the court held that use of a two-way mirror in a dressing room was not an invasion of privacy because customers do not have a legitimate expectation of privacy in light of signs posted in the dressing room indicating there was surveillance. It is not clear how this case is applicable to the instant facts, it is undisputed that Plaintiff was unaware of Defendant's use of the key logger.

Defendant also cites *Saldana v. Kelsey-Hayes Company*, 178 Mich.App. 230, 443 N.W.2d 382 (Mich.App.1989), where the court found an employer's use of a high powered lens to look into an employee's home for purposes of determining whether he was disabled was not an invasion of privacy. The court found the plaintiff did not have a right to privacy because the surveillance "involved matters which defendants had a legitimate right to investigate." *Id.* at 234, 443 N.W.2d 382. The court found that an employer has a legitimate right to investigate suspicions that an employee's work-related disability is a pretext. *Id.* at 235, 443 N.W.2d 382. This case is not dispositive of Plaintiff's claim.

Defendant asserts that he had a right to monitor Plaintiff's computer activities in the interests of himself, Plaintiff, and their children. [Motion, p. 26]. However, Plaintiff presents evidence that Defendant continued to access her private email after the divorce, and regarding matters that were no longer of Defendant's concern. [Plaintiff's Exhibit A]. In general, Plaintiff had a right to privacy in her private email account.

Plaintiff raises an issue of fact regarding whether Defendant Bailey's use of a key logger to learn her email and messaging passwords so that he could access her private correspondence was objectionable to a reasonable

Bailey v. Bailey, Not Reported in F.Supp.2d (2008)

man. See *Saldana*, 178 Mich.App. at 234, 443 N.W.2d 382 (“[w]hether the intrusion is objectionable to a reasonable person is a factual question best determined by a jury.”). Defendant Bailey is not entitled to summary judgment on this claim.

2. Public disclosure of private facts

*11 “A cause of action for public disclosure of embarrassing private facts requires (1) the disclosure of information, (2) that is highly offensive to a reasonable person, and (3) that is of no legitimate concern to the public.” *Doe*, 212 Mich.App. at 80, 536 N.W.2d 824. Further, as the name of the claim implies, the information must be disclosed to the public. *Duran v. The Detroit News, Inc.*, 200 Mich.App. 622, 631, 504 N.W.2d 715 (Mich.App.1993).

The alleged “public” disclosure of the information contained in Plaintiff’s emails consists of Defendant Pope’s use of the emails to impeach Plaintiff’s testimony during a custody hearing, although he did not admit them into evidence; copies were sent as exhibits to Plaintiff’s attorney, Defendant Kozyra; and the emails were summarized in response to a motion by Plaintiff. None of these is sufficient to support Plaintiff’s claim for invasion of privacy based on public disclosure of private facts.

The information disclosed, regarding Plaintiff’s sexual relations, were private facts. “Sexual relations, for example, are normally entirely private matters.” *Doe*, 212 Mich.App. at 82, 536 N.W.2d 824 (citation omitted). However, the information must be of no legitimate concern to the public. All of the disclosures were in the context of a court case to determine the custody of the parties three children. Where the state is required to determine the custody of children during a divorce, the fitness of a person to parent is of legitimate concern to the public. Thus, this was not “unreasonable publicity.” See *Doe*, 212 Mich.App. at 81, 536 N.W.2d 824.

Accordingly, Defendants are entitled to summary judgment on this claim.

G. Intentional Infliction of Emotional Distress

Plaintiff alleges a claim of intentional infliction of emotional distress against all Defendants. In order to establish her claim, Plaintiff must prove: (1) extreme and outrageous conduct; (2) intent or recklessness; (3) causation; and (4) severe emotional distress. *Lewis*, 258 Mich.App. at 196, 670 N.W.2d 675. “Liability attaches only when a plaintiff can demonstrate that the defendant’s

conduct is ‘so outrageous in character, and so extreme in degree, as to go beyond all possible bounds of decency, and to be regarded as atrocious and utterly intolerable in a civilized community.’” *Id.* (citation omitted). “The test to determine whether a person’s conduct was extreme and outrageous is whether recitation of the facts of the case to an average member of the community ‘would arouse his resentment against the actor, and lead him to exclaim, Outrageous!’” *Id.* (citation omitted).

In this case, Defendants’ conduct of using a key logger to obtain Plaintiff’s passwords in order to gain access to her email and messaging accounts, and then using copies of those documents in divorce and custody proceedings is not extreme and outrageous conduct. A husband snooping in his wife’s email, after learning that she was engaging in sexual discussions over the internet while the children may have been present, and using damaging emails in divorce and custody proceedings can hardly be considered “atrocious and utterly intolerable in a civilized society.” Consistent with the discussion above regarding Plaintiff’s invasion of privacy claim, Defendant Bailey’s method of garnering the information may be objectionable to a reasonable man, that is for the jury to decide, but his conduct does not “go beyond all possible bounds of decency.”

*12 Defendants are entitled to summary judgment on Plaintiff’s claim for intentional infliction of emotional distress.

H. Subject Matter Jurisdiction

The only remaining claim against Defendant Kozyra, is for professional negligence based on his representation of Plaintiff in her state court proceedings. “[F]ederal courts have an independent obligation to investigate and police the boundaries of their own jurisdiction.” *Douglas v. E.F. Baldwin & Associates, Inc.*, 150 F.3d 604, 607 (6th Cir.1998). Although Kozyra has not brought a motion before this Court, the Court may review the issue of subject matter jurisdiction sua sponte.

Plaintiff’s claim arises under state law, thus the basis for subject matter jurisdiction is supplemental jurisdiction. 28 U.S.C. § 1367. Section 1367(a) provides that the court has supplemental jurisdiction “over all other claims that are so related to claims in the action within such original jurisdiction that they form part of the same case or controversy.” See *United Mine Workers of America v. Gibbs*, 383 U.S. 715, 725, 86 S.Ct. 1130, 16 L.Ed.2d 218 (1966) (In order to exercise pendent jurisdiction, “[t]he state and federal claims must derive from a common nucleus of operative fact.”). Plaintiff’s professional

Bailey v. Bailey, Not Reported in F.Supp.2d (2008)

negligence claim is not a part of the same “case or controversy” and does not arise from a “common nucleus of operative fact” as the claims pertaining to Defendants’ access and use of Plaintiff’s private emails.

Accordingly, this Court cannot exercise supplemental jurisdiction over Plaintiff’s professional negligence claim. To the extent the Court could exercise jurisdiction over the claim, it declines to do so under 28 U.S.C. § 1367(c). Therefore, because this was the only remaining claim against him, Defendant Andrew Kozyra is dismissed from this action.

IV. CONCLUSION

For the foregoing reasons, the Court **GRANTS** Defendant Todd Pope’s Motion for summary judgment; and **GRANTS** in part, and **DENIES** in part, Defendant Jeffrey Bailey’s Motion for summary judgment. Summary

End of Document

judgment is granted on Plaintiff’s claims for: (1) violation of 18 U.S.C. § 2511; (2) violation of 18 U.S.C. § 2512; (3) MCL § 750.539a, et seq.; (4) MCL § 750.540; (5) invasion of privacy against Defendant Pope based on intrusion upon seclusion; (6) invasion of privacy based on public disclosure; and (7) intentional infliction of emotional distress. Summary judgment is denied on Plaintiff’s claims for: (1) violation of 18 U.S.C. § 2701 against Defendant Bailey; and (2) invasion of privacy against Defendant Bailey based on intrusion upon seclusion. Additionally, Defendant Andrew Kozyra is **DISMISSED** from this action.

IT IS SO ORDERED.

All Citations

Not Reported in F.Supp.2d, 2008 WL 324156

© 2015 Thomson Reuters. No claim to original U.S. Government Works.

Ideal Aerosmith, Inc. v. Acutronic USA, Inc., Not Reported in F.Supp.2d (2007)
87 U.S.P.Q.2d 1341

2007 WL 4394447
Only the Westlaw citation is currently available.
United States District Court,
E.D. Pennsylvania.

IDEAL AEROSMITH, INC., Plaintiff,
v.
ACUTRONIC USA, INC., et al., Defendants.
Civil Action No. 07-1029. | Dec. 13, 2007.

Attorneys and Law Firms

Roy E. Leonard, Stonecipher, Cunningham, Beard & Schmitt, Pittsburgh, PA, for Plaintiff.

Leland P. Schermer, Leland Schermer & Associates, Pittsburgh, PA, for Defendants.

misappropriation of trade secrets, unfair competition and civil conspiracy.

I. LEGAL STANDARD

In deciding a motion to dismiss under Fed.R.Civ.P. 12(b)(6), all factual allegations, and all reasonable inferences therefrom, must be accepted as true and viewed in a light most favorable to the plaintiff. *Haspel v. State Farm Mut. Auto. Ins. Co.*, 2007 WL 2030272, at *1 (3d Cir. July 16, 2007). However, “[f]actual allegations must be enough to raise the right to relief above the speculative level.” *Bell Atlantic Corp. v. Twombly*, --- U.S. ---, 127 S.Ct. 1955, 167 L.Ed.2d 929 (2007). In order to survive a motion to dismiss, the complaint must “contain either direct or inferential allegations respecting all the material elements necessary to sustain recovery under some viable legal theory.” *Id.* at 1969.

OPINION and ORDER OF COURT

AMBROSE, Chief Judge.

SYNOPSIS

*1 Plaintiff Ideal Aerosmith, Inc. (“Plaintiff” or “Ideal”) asserts claims under federal and Pennsylvania state wiretapping and stored communications laws and additional state law claims for violation of Pennsylvania’s uniform trade secrets act, wrongful procurement/conversion of business information, civil conspiracy, and unfair competition. Defendants Acutronic USA, Inc., Michael H. Swamp and Carl N. Hockenberry (collectively, “Acutronic”), Acutronic Schweiz AG, Acutronic Group¹, Jung Technologies Holding AG and Thomas W. Jung (collectively, the “Swiss Defendants”) have moved to dismiss the Complaint under Federal Rule of Civil Procedure 12(b)(6) for failure to state a claim [Docket Nos. 5 and 11]. For the reasons set forth below, I dismiss Counts 1, 2, 4 and 5 of the Complaint setting forth claims under federal and state wiretapping and stored communications laws and Count 6 of the Complaint alleging wrongful procurement/conversion of business information. I deny Defendants’ motions to dismiss Counts 3, 7 and 8 of the Complaint alleging

II. DEFENDANTS’ MOTIONS TO DISMISS

A. ALLEGATIONS OF THE COMPLAINT

Plaintiff Ideal is a leading manufacturer and supplier of aerospace test equipment, including motion simulators for inertial guidance testing, gyro test systems and missile simulators, in the United States and international markets. Among its products, Plaintiff developed and manufactures the AERO 4000 motion controller.

Defendants, located in the United States and Switzerland, also manufacture and supply aerospace test equipment and motion simulators. They are Ideal’s principal competitors in the domestic and international aerospace motion controller market. Defendants Acutronic and Acutronic Schweiz manufacture and sell a motion controller system known as the ACUTROL 3000, which competes with Ideal’s AERO 4000.

Non-party Carco Electronics (“Carco”) was the only company that competed to a significant degree with Ideal and Defendants in the motion simulator market. However, Carco entered into bankruptcy protection as a debtor-in-possession under Chapter 11 of the Bankruptcy Code. Pursuant to its plan of reorganization, which was filed in the United States Bankruptcy Court for the Western District of Pennsylvania, Carco was required to market

Ideal Aerosmith, Inc. v. Acutronic USA, Inc., Not Reported in F.Supp.2d (2007)

87 U.S.P.Q.2d 1341

and sell substantially all of its assets free and clear of liens.

*2 On December 17, 2004, Carco ceased all its operations and terminated all of its production workers at its two operating facilities in Pittsburgh, Pennsylvania and Menlo Park, California. On December 31, 2004, Ideal entered into an asset purchase agreement with Carco. On January 2, 2005, Ideal hired most of Carco's former employees in order to continue Carco's operations and preserve its assets pending the Bankruptcy Court's approval of the sale. Ideal also took possession of Carco's facilities and began operating Carco's business and filling outstanding orders. During this time, the former Carco employees who had been hired by Ideal continued to use their Carco e-mail addresses, which utilized the domain names of "carco-east.com" for the Pittsburgh office and "carcoelect.com" for the Menlo Park office.

On February 1, 2005, the Bankruptcy Court conducted an auction-type sale of Carco's assets under section 363 of the Bankruptcy Code. Acutronic outbid Ideal and Carco's secured creditor and purchased substantially all of Carco's assets on a non-warranty 'as is, where-is' basis. Within a day following the sale hearing, Ideal tendered possession of the Carco facilities to Acutronic, and all of Ideal's employees, including the former Carco employees, left the Carco facilities. As of February 2, 2005, Acutronic exercised control of Carco's assets, including the Carco e-mail addresses of all of Carco's former employees. On or about February 15, 2005, Acutronic and Carco closed on the asset sale and Acutronic became the owner of Carco's assets.

Shortly after the sale hearing on February 1, 2005, all of the former Carco employees hired by Ideal were assigned new "Ideal" e-mail addresses. These addresses all contained the domain name "idealaero.com." Plaintiff alleges that, despite providing new "Ideal" e-mail addresses, former Carco employees, now employed by Ideal, and third parties doing business with Ideal inadvertently continued to send communications using the old Carco e-mail addresses with the Carco domain name. According to Plaintiff, Acutronic, which now owned the Carco servers, caused the Carco servers to redirect those e-mail messages to an Acutronic server. Acutronic then read the messages, some of which contained Ideal trade secrets and confidential business information, including information related to the marketing and sale of Ideal's Aero 4000, and shared the contents of the messages and/or forwarded the messages to and among the Defendants. Acutronic did not disable the old Carco addresses, did not inform the senders that the addresses were no longer valid, and did not forward the messages to the intended recipients.

Plaintiff alleges that these actions constitute a violation of the Federal Wiretapping Act, 18 U.S.C. secs. 2510 *et seq.*, the Federal Stored Communications Act, 18 U.S.C. secs. 2701 *et seq.*, Pennsylvania Uniform Trade Secrets Act, 12 Pa.C.S. secs. 5308 *et seq.*, Pennsylvania Wiretapping Act, 18 Pa.C.S. secs. 5701 *et seq.*, Pennsylvania Wiretapping Act-Stored Communications, 18 Pa.C.S. secs. 5741 *et seq.*, and Pennsylvania common law of wrongful procurement/conversion of business information, civil conspiracy and unfair competition.

B. WIRETAPPING AND STORED COMMUNICATIONS CLAIMS-COUNTS 1, 2, 4 AND 5

1. Statute of Limitations

*3 The statute of limitations for claims brought under the Federal Wiretapping and Stored Communications Acts is two years from the date "the claimant first has a reasonable opportunity to discover the violation." 18 U.S.C. § 2520(e); 18 U.S.C. § 2707(f). Pennsylvania's wiretapping and stored communications statutes also have two-year statutes of limitations. 18 Pa.C.S. § 5474(e); 42 Pa.C.S. § 5524(7). Defendants argue that since Plaintiff has alleged that the interceptions began on or about February 2, 2004, and this action was not commenced until July 23, 2007, the claims are time-barred.

"In ruling on a motion to dismiss on statute of limitations grounds, the Court may not look beyond the face of the complaint. Thus, 'a 12(b)(6) motion should not be granted on limitations grounds unless the complaint facially shows noncompliance with the limitations period.' *Giusto v. Ashland Chem. Co.*, 994 F.Supp. 587, 594 (E.D.Pa.1998) (quoting *Clark v. Sears Roebuck & Co.*, 816 F.Supp. 1064, 1067 (E.D.Pa.1993)); see also, *Hunt v. PA Dep't of Corrections*, 2006 WL 676222, at *1 (3d Cir. Mar.17, 2006) ("A complaint may not be dismissed under Rule 12(b)(6) as untimely under the relevant statute of limitations unless it is plain from the face of the complaint that it was not timely filed."); *Fralin v. C and D Sec., Inc.*, 2007 WL 1576464, at *4 (E.D.Pa. May 30, 2007) (refusing to consider allegations outside the complaint for statute of limitations determination).

Plaintiff correctly argues that the statute of limitations on its wiretapping and stored communications claims does not begin to run until it discovered or with the exercise of reasonable diligence should have discovered the acts constituting the alleged violation. See, e.g., *Directv, Inc. v. Rodkey*, 369 F.Supp.2d 587, 598 (W.D.Pa.2005) (discovery rule applicable to wiretapping claims).

Ideal Aerosmith, Inc. v. Acutronic USA, Inc., Not Reported in F.Supp.2d (2007)

87 U.S.P.Q.2d 1341

Here, the Complaint does not allege when Ideal discovered the purported wiretapping and accessing of stored electronic communications. Moreover, Ideal alleges that the conduct of Defendants is ongoing. Accordingly, at this stage of the proceedings, questions of fact preclude dismissal of Plaintiff's wiretapping and electronic storage claims on statute of limitations grounds.

2. Adequacy of Pleading-Wiretapping Claims

Plaintiffs' first and fourth claims arise under the Federal Wiretapping Act, 18 U.S.C. §§ 2510 *et seq.* and its Pennsylvania counterpart, the Pennsylvania Wiretapping Act, 18 Pa.C.S. §§ 5701 *et seq.* The Pennsylvania act tracks the language set forth in the Federal Act, and has been interpreted identically. *See Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107, 113 n. 6 (3d Cir.2004) (Pennsylvania statute "interpreted in the same way as the ECPA, [and] the analysis and conclusions in the text apply equally to this state law claim"). Plaintiff alleges that Defendants violated the Acts "[b]y unlawfully intercepting, disclosing and using Ideal's emails." (Complaint, ¶¶ 33, 39.)

*4 Title I of the Electronic Communications Privacy Act of 1986 (the "ECPA" or "Wiretap Act"), which amended the Wiretap Act of 1968, makes it an offense to "intentionally intercept[], endeavor[] to intercept, or procure[] any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication...." 18 U.S.C. § 2511(1); *see also*, *United States v. Councilman*, 418 F.3d 67 (1st Cir.2005) (discussing the legislative history of the ECPA). In addition, liability under the Wiretap Act may arise from the disclosure of, attempt to disclose, use of or attempt to use, the contents of any communication while knowing or having reason to know that such contents were obtained through an interception violating the Act. 18 U.S.C. § 2511(1)(c)-(d). "Intercept" is defined by the Wiretap Act as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4).

Accordingly, in order to state a claim under the Wiretap Act, a plaintiff must allege that a communication was intentionally intercepted through the use of a device. It follows that, absent an interception, neither the disclosure nor use of the contents of the communication violates the Wiretap Act. *Wesley College v. Pitts*, 974 F.Supp. 375, 381 (D.Del.1997), *aff'd*, 172 F.3d 861 (3d Cir.1998). "The Court need not accept a conclusory allegation that conduct alleged in the complaint constituted an interception under the Wiretap Act." *Crowley v.*

Cybersource Corp., 166 F.Supp.2d 1263, 1268 (N.D.Ca.2001).

In support of its wiretapping claims, Ideal has alleged that, after Acutronic purchased Carco, certain e-mail messages (the "Ideal Emails") were sent by Ideal's employees, including former Carco employees hired by Ideal, and by third parties conducting business with Ideal, to web addresses utilizing the Carco domain name. These e-mail messages were received by the Carco servers, now owned by Acutronic, and "redirected" by Acutronic to its own servers and/or forwarded to and among the other Defendants.

These allegations do not state a claim of wiretapping. As an initial matter, Plaintiff has standing to assert claims only with respect to those communications sent by Plaintiff and its employees, not with respect to those communications sent by third parties. *See Klump v. Nazareth Area Sch. Dist.*, 425 F.Supp.2d 622, 633 (E.D.Pa.2006) ("The intended recipient of an intercepted communication ... has no standing to raise claim under [the Pennsylvania Wiretap Act]. Rather, "that cause of action belongs only to the person with whom the communication originated...."). More significantly, Plaintiff has failed to allege the use of a device to intercept the communications. *See Wesley College v. Pitts*, 974 F.Supp. at 385 (interception does not occur absent the use of a device); *Commonwealth v. Proetto*, 771 A.2d 823, 832 (Pa.Super.Ct.2001) (under Pennsylvania Wiretap Act, "intercept" requires the contemporaneous acquisition of the communication through the use of a device), *aff'd*, 575 Pa. 511, 837 A.2d 1163 (Pa.2003). The drive or server on which an e-mail is received does not constitute a device for purposes of the Wiretap Act. *See Crowley*, 166 F.Supp.2d at 1269.

*5 In *Crowley*, the plaintiffs purchased items from Amazon.com. As part of their transactions, they transferred certain information about themselves, including identity and credit information. 166 F.Supp.2d at 1266. Amazon, in turn, relayed this information to CyberSource for purposes of verifying the plaintiffs' credit. *Id.* Cyberspace compiled this information, as well as information on those purchasers acquired from other vendors, into a database profiling the purchasers. *Id.* The plaintiffs alleged that Amazon intercepted their communications, disclosed the contents to Cyberspace and used the contents to create profiles of the purchasers, all in violation of the Wiretap Act. *Id.* at 1267.

The District Court granted Amazon's motion to dismiss the claim under the Wiretap Act.

Ideal Aerosmith, Inc. v. Acutronic USA, Inc., Not Reported in F.Supp.2d (2007)

87 U.S.P.Q.2d 1341

Amazon did not, however, "intercept" the communication within the meaning of the Wiretap Act, because Amazon did not acquire it using a device other than the drive or server on which the e-mail was received....Amazon acted as no more than the second party to a communication. This is not an interception as defined by the Wiretap Act. [Plaintiff's] argument, moreover, would result in an untenable result. Holding that Amazon, by receiving an e-mail, intercepted a communication within the meaning of the Wiretap Act would be akin to holding that one who picks up a telephone to receive a call has intercepted a communication and must seek safety in an exemption to the Wiretap Act. Such a result would effectively remove from the definition of intercept the requirement that the acquisition be through a "device."

Id. at 1269; *see also*, *Hall v. EarthLink Network, Inc.*, 396 F.3d 500, 504 (2d Cir.2005) (Earthlink's continued receipt and retention on its system of e-mails sent to subscriber's closed account did not constitute the use of a device resulting in an interception under the Wiretap Act).

Here, there is no dispute that the Ideal E-mails were sent directly to Carco's server, now owned by Acutronic. Acutronic employed no device to acquire these e-mails, but was merely, as owner of Carco's system, a direct party to the communication. While Ideal complains that Acutronic was not the intended recipient of the communication, that argument has no legal bearing where the communication was nonetheless sent to Carco/Acutronic. *See Proetto*, 771 A.2d at 832 (no wiretapping violation despite the fact that police officer, rather than defendant, received the call since "[t]he Wiretapping Act is not intended to prevent a telephone user from misrepresenting his identity").²

Moreover, even if Acutronic's acquisition of the e-mails constituted an "interception" for purposes of the Wiretap Act, Acutronic is exempt under section 2511(2), which allows an "officer, employee or agent of a provider of wire or electronic service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose or use that communication in the

normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service." 18 U.S.C. § 2511(2); *see also*, 18 Pa.C.S.A. § 5704(1) (same). In *Freedom Calls Foundation v. Bukstel*, 2006 WL 845509, at *27 (E.D.N.Y. Mar.3, 2006), the defendant, a former employee who had established a competing business, asserted a counterclaim seeking injunctive relief to prevent the plaintiff, his former employer, from continuing to monitor the defendant's prior e-mail address at the plaintiff's company. The District Court held that the plaintiff had a right under the Wiretap Act to continue to monitor e-mails sent to the former employee. "Plaintiff has the right to "intercept," that is, receive and review future e-mails sent to the ebukstel@freedomcalls.org account, so long as it does so in the normal course of business, because Plaintiff is an employer and monitoring is necessary to ensure that current and prospective Supporter and Client email messages are answered in a timely manner." 2006 WL 845509, at *27.

*6 Based on the allegations of the Complaint, Acutronic purchased the assets of Carco. As the purchaser, Acutronic became the successor-in-interest to Carco's business, and had the right to monitor communications received by Carco via Carco's server. Accordingly, even if the communications were intercepted, Acutronic is exempt from liability under the Wiretap Act for the alleged conduct.

For the foregoing reasons, I dismiss Counts 1 and 4 of the Complaint.

3. Adequacy of Pleading-Stored Communications Claims

Plaintiff's second and fifth claims arise under the Federal Stored Communications Act, 18 U.S.C. §§ 2701 *et seq.*, and the Stored Communication provision of the Pennsylvania Wiretapping Act, 18 Pa.C.S. §§ 5741 *et seq.* The same allegations upon which the wiretapping claims discussed above rely are also the basis of Plaintiff's stored communications claims.

Title II to the ECPA, the Stored Wire and Electronic Communications and Transactional Records Access (the "Stored Communications Act"), 18 U.S.C. § 2701, provides that "whoever (1) intentionally accesses without authorization a facility through which an electronic communication service is provided ... and thereby obtains, alters or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished...." Section 2707 provides for a

Ideal Aerosmith, Inc. v. Acutronic USA, Inc., Not Reported in F.Supp.2d (2007)

87 U.S.P.Q.2d 1341

private right of action for injunctive relief and damages for violations of the provision. 18 U.S.C. § 2707(a)-(c). The language of the Pennsylvania statute, 18 Pa.C.S. § 5741, mirrors the federal statute and is interpreted accordingly. *Fraser*, 352 F.3d at 114 n. 9.

The general purpose of the Stored Communications Act was to “create a cause of action against ‘computer hackers (e.g. electronic trespassers).’ ” *International Ass’n of Machinists and Aerospace Workers v. Werner-Masuda*, 390 F.Supp.2d 479, 495 (D.Md.2005) (quoting *Sherman & Co. v. Salton Maxim Housewares, Inc.*, 94 F.Supp.2d 817, 820 (E.D.Mich.2000)). This purpose is consistent with the broad exemption provided by Title II with respect to “conduct authorized by the person or entity providing a wire or electronic communications service.” 18 U.S.C. § 2701(c) (1). Numerous courts have found that employers which provide their employees with “the ability to send or receive electronic communications” are “person[s] or entit[ies] providing a wire or electronic communications service” for purposes of the exemption. *See, e.g., Fraser*, 352 F.3d at 115 (insurance company which administered e-mail system for its agents was a provider); *Freedom Calls Foundation*, 2006 WL 845509, at *27 (foundation a provider of service); *Bohach*, 932 F.Supp. at 1237 (city is the provider of electronic communications service to police department since police department’s terminals, computer and software enable them to send or receive electronic communications).

A defendant who is a provider of electronic communication service is immune from liability under § 2701. In *Fraser*, the Third Circuit held that an employer which provided e-mail service to its employees was exempt from liability under Title II when it searched and retrieved from its system e-mails sent and received by its employee. 352 F.3d at 115. The Third Circuit relied on the District Court of Nevada’s opinion in *Bohach v. City of Reno*, 932 F.Supp. 1232, 2336 (D.Nev.1996), which held that “ § 2701(c) (1) allows service providers to do as they wish when it comes to accessing communications in electronic storage.” *See also, Freedom Calls Foundation*, 2006 WL 845509, at *27 (“Plaintiff has the right to search these stored e-mails as the need arises because Plaintiff provided Defendant with the ability to send and receive electronic communications.”); *In re Amercian Airlines, Inc. Privacy Litig.*, 370 F.Supp.2d 552, 557 n. 8 (N.D.Tex.2005) (claim under 2701 “would seem to make little sense since American would apparently have plenary authority to access its own facility”).

*7 The Complaint alleges that Acutronic purchased the assets of Carco, including “the e-mail addresses of all of Carco’s former employees.” (Complaint, ¶ 21.) Thus, Carco’s computers, servers and software all became the

property of Acutronic, which became responsible for administering it. Accordingly, Acutronic is a provider within the meaning of 2701(c) and is exempt from liability for accessing e-mails sent to and stored in its facilities.

Plaintiff’s allegations that Defendants disclosed and used the content of those communications do not save its invalid claim under § 2701. “Section 2701 does not proscribe unauthorized use or disclosure of information obtained from authorized access to a facility.” *In re American Airlines, Inc. Privacy Litig.*, 370 F.Supp.2d at 559; *see also, International Ass’n of Machinists and Aerospace Workers*, 390 F.Supp.2d at 499 (Title II does “not prohibit the unauthorized disclosure or use of information, but rather unauthorized access. Nor [do its] terms proscribe authorized access for unauthorized or illegitimate purposes.”); *Sherman & Co. v. Salton Maxim Housewares, Inc.*, 94 F.Supp.2d 817, 820 (E.D.Mich.2000) (disclosure of information to a competitor does not state a claim under § 2701); *Wesley*, 974 F.Supp. at 389 (“Title II prohibits unauthorized access to stored electronic communications, but does not censure the disclosure or use of the contents of those stored communications....”). Since Acutronic, as a provider of the communications service, has the unfettered right to access communications stored on its system, it also cannot be liable under § 2701 for the use or disclosure of the contents of those communications.

Based on the foregoing, I find that Plaintiff has failed to state a claim under section 2701 of the Stored Communications Act, as well as its Pennsylvania counterpart. Accordingly, I dismiss counts 2 and 5 of the Complaint.

C. PLAINTIFF’S STATE LAW CLAIMS

1. Pennsylvania Uniform Trade Secrets Act

Plaintiff’s third claim arises under the Pennsylvania Uniform Trade Secrets Act (“PUTSA”), 12 Pa.C.S. §§ 5308 *et seq.* Plaintiff alleges that by “unlawfully intercepting, disclosing and using Ideal’s Emails, Defendants violated” the PUTSA. (Complaint ¶ 39.) Defendants argue that this claim must be dismissed because “Ideal never identifies what comprises the alleged trade secrets or what steps it took to make the alleged trade secret information a trade secret.” (Def. Mem. at 18.) Defendants further argue that there can be no trade secret as a matter of law because Plaintiff disclosed the information, even if accidentally or inadvertently, and that a claim under the PUTSA requires

Ideal Aerosmith, Inc. v. Acutronic USA, Inc., Not Reported in F.Supp.2d (2007)

87 U.S.P.Q.2d 1341

a wrongful act in acquiring the e-mails. (Def. Reply Mem. at 5.)

The PUTSA defines a "trade secret" as "[i]nformation, including a formula, drawing, pattern, compilation including a customer list, program, device, method, technique or process that (1) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use[; and] (2)[i]s the subject of efforts that are reasonable under the circumstances to maintain its secrecy." 12 Pa.C.S.A. § 5302. The PUTSA defines "misappropriation" as, in relevant part: "(2) disclosure or use of a trade secret of another without express or implied consent by a person who ... (iii) before a material change of his position, knew or had reason to know that it was a trade secret and that knowledge of it had been acquired by accident or mistake." *Id.*

*8 Defendants' argument that Plaintiff has failed adequately to allege what comprises the trade secrets is incorrect. In paragraph 25 of its Complaint, Plaintiff identified the trade secrets as relating to, "information concerning the development, marketing and sale of Ideal's Aero 4000 motion controller, customer communications and other property." Plaintiff further alleged that the Ideal Emails contained trade secret and confidential business information and other property "including proprietary development specifications for Ideal's AERO 4000, pricing data, marketing information, product bid information, and customer communications." (Complaint, § 27.) This constitutes adequate identification of the trade secret material for pleading purposes. *See Freedom Med. Inc. v. Gillepsie*, 2007 WL 2480056, at *22 (E.D.Pa. Aug.29, 2007) (claim for misappropriation of trade secrets need not be pleaded with particularity).

Defendants' remaining arguments do not warrant dismissal of Plaintiff's trade secrets claim. As an initial matter, Plaintiff correctly points out that the case law relied upon by Defendants interprets Restatement of Torts § 757, rather than the PUTSA. *See, Frank W. Winne and Son, Inc. v. Palmer*, 1991 WL 155819, at *3 (E.D.Pa. Aug.7, 1991); *Defiance Button Machine Co. v. C & C Metal Prods. Corp.*, 759 F.2d 1053 (2d Cir.), *cert. denied*, 474 U.S. 844, 106 S.Ct. 131, 88 L.Ed.2d 108 (1985). In any event, even under that case law, whether a plaintiff has taken sufficient measure to protect its trade secrets is a question of fact. *See, e.g., Frank W. Winne and Son, Inc.*, 1991 WL 155819, at *3. Here, Defendant does not claim that it learned or could have learned Plaintiff's trade secrets in any manner except by reading the Ideal Emails sent to old Carco e-mail addresses. Plaintiff alleges that,

upon Carco's sale to Acutronic, Plaintiff provided new Ideal e-mail addresses to the former Carco employees. *Compare Defiance Button Machine Co.*, 759 F.2d at 1063-64 (no protection for trade secret information left on hard drive of computer transferred to defendant as part of asset sale). Moreover, Plaintiff has also alleged that some of the Ideal Emails acquired by Defendants were sent by Plaintiff's customers and/or potential customers. (Complaint, ¶ 25.) Again, the record at this stage does not allow me to determine as a matter of law that Plaintiff failed to take adequate measures to protect those trade secrets in the hands of third parties. *See CDI Internat'l, Inc. v. Marck*, 2005 WL 327536, at *2 (E.D.Pa. Feb.8, 2005) (denying motion to dismiss where "record before the Court at this early stage of the litigation is not developed enough to conclude that CDI failed to take reasonable steps to protect its trade secrets and thus forfeited those trade secrets").

Finally, a plaintiff can state a claim for misappropriation of trade secrets under Pennsylvania law even where the trade secret was acquired by mistake rather than misconduct. To state a claim for misappropriation under the PUTSA, the plaintiff need only allege that the defendant used or disclosed information that it knew or had reason to know was a trade secret and that the defendant had acquired such information by accident or mistake. 12 Pa.C.S.A. § 5302; *see also, B & B Microscopes v. Armogida*, 2007 WL 2814595, at *11 (W.D.Pa. Sept.25, 2007) ("The Pennsylvania Uniform Trade Secrets Act, 12 Pa.C.S.A. § 5301 et seq. makes it unlawful to disclose or use the trade secret without consent."); *H2Ocean, Inc. v. Schmitt*, 2006 WL 1835974, at *3 (N.D.Fl. June 30, 2006) (interpreting an identical trade secret statute and denying motion to dismiss complaint "[s]ince a defendant can commit theft of trade secrets without acquiring the trade secrets in question by improper means"), *appeal dismissed*, 208 Fed.Appx. 843 (Fed.Cir.2006).³ Here, Plaintiff has alleged that Acutronic acquired Plaintiff's trade secrets by mistake when they were inadvertently sent to old Carco e-mail addresses, and that Defendants disclosed and used these trade secrets to compete with Plaintiff. Accordingly, Plaintiff has stated a claim for violation of Pennsylvania's Uniform Trade Secrets Act.

2. Wrongful Procurement/ Conversion of Business Information

*9 Count 6 of the Complaint alleges a claim for wrongful procurement/conversion of business information. Specifically, Plaintiff alleges that "Defendants used improper means to wrongfully procure and/or convert Ideal's confidential and valuable business information

Ideal Aerosmith, Inc. v. Acutronic USA, Inc., Not Reported in F.Supp.2d (2007)

87 U.S.P.Q.2d 1341

contained in Ideal's Emails." (Complaint, ¶ 48.) Defendants argue that, since Plaintiff has not stated a valid claim under the federal or state wiretapping or stored communications statutes, then Plaintiff's claim for wrongful procurement must also fail. I agree with Defendants.

Pennsylvania courts have recognized as actionable conduct prohibited under Section 759 of the Restatement of Torts. *See Pestco, Inc. v. Associated Prods., Inc.*, 880 A.2d 700, 708 (Super.Ct.2005); *Den-Tal-Ez, Inc. v. Siemens Capital Corp.*, 389 Pa.Super. 219, 566 A.2d 1214, 1231 (Pa.Super.Ct.1989). Section 759 provides: "One who, for the purpose of advancing a rival business interest, procures by improper means information about another's business is liable to the other for the harm caused by his possession, disclosure or use of the information." *Pestco, Inc.*, 880 A.2d at 709. As Defendants have argued, a claim brought under this theory requires acquisition of confidential business information through misconduct. *See Den-Tal-Ez, Inc.*, 566 A.2d at 253-54 ("[t]he requirement that the defendant procure the information by improper means is also squarely fulfilled in this case").

The sole 'improper means' alleged by Plaintiff is through violations of the federal and state wiretapping and stored communications acts. Since I dismissed Plaintiff's claims under those statutes in section II(B) above, I accordingly dismiss Plaintiff's sixth claim alleging wrongful procurement.

3. Unfair Competition

Count 8 of the Complaint alleges that "[b]y engaging in the conduct described above, Defendants have unlawfully and without privilege engaged in unfair competition under the common law of the Commonwealth of Pennsylvania to the detriment of Ideal in violation of the law." (Complaint, ¶ 56.) As with the wrongful procurement claim discussed above, Defendants argue that Plaintiff has failed to state a claim for unfair competition because it has failed to allege that Defendants procured the information through improper means. With respect to this claim, I disagree with Defendants' interpretation of Pennsylvania law..

"A claim for unfair competition may be based on conduct that is otherwise actionable at common law." *Brett Senior & Assocs., P.C. v. Fitzgerald*, 2007 WL 2043377, at * 8 n. 12 (E.D.Pa. July 13, 2007) (unfair competition claim dependent on dismissed misappropriation claim must also fail); *see also, Lakeview Ambulance and Med. Svcs., Inc. v. Gold Cross Ambulance and Med. Svc., Inc.*, 1995 WL

842000, at *1 (Pa.Comm.Pl. Oct. 18, 1995) ("The doctrine of unfair competition extends to the misappropriation for the commercial advantage of a benefit or a property right belonging to another.").

*10 While I have dismissed Counts 1, 2, 4, 5 and 6, Plaintiff's third claim for misappropriation of trade secrets remains. Accordingly, I deny Defendants' motions to dismiss Count 8 alleging unfair competition.

4. Civil Conspiracy

Count 7 of the Complaint alleges a claim for civil conspiracy under Pennsylvania common law. To plead a claim for civil conspiracy, a plaintiff must allege: "(1) the persons combined with a common purpose to do an unlawful act or to do a lawful act by unlawful means or unlawful purpose, (2) an overt act in furtherance of the common purpose has occurred, and (3) the plaintiff has incurred actual legal damage." *Rouse v. II-VI, Inc.*, 2007 WL 1007925, at *14 (W.D.Pa. Mar.30, 2007). "Simply alleging the existence of an agreement or conspiracy is not enough" to survive a motion to dismiss. *Kist v. Fatula*, 2007 WL 2404721, at *9 (W.D.Pa. Aug.17, 2007). Rather, a plaintiff must "allege particularized facts, such as those addressing the period of the conspiracy, the object of the conspiracy, and certain actions of the alleged conspirators taken to achieve that purpose." *Bair v. Purcell*, 500 F.Supp.2d 468, 500 (M.D.Pa.2007).

I find that Plaintiff has met its burden of pleading a claim of civil conspiracy, albeit barely. Plaintiff has alleged a conspiracy beginning on or about February 2005, between Acutronic and the Swiss Defendants, to use and disclose the Ideal E-mails involving Plaintiff's trade secrets and confidential business information, in order to more effectively compete against Plaintiff in the United States and European markets. (Complaint, ¶¶ 24, 27.) Of course, this civil conspiracy claim only survives with respect to those state law claims that have not been dismissed, i.e. misappropriation of trade secrets and unfair competition. *See Boyanowski v. Capital Area Intermediate Unit*, 215 F.3d 396, 406 (3d Cir.) ("We are unaware of any jurisdiction that recognizes civil conspiracy as a cause of action requiring no separate tortious conduct."), *cert. denied*, 531 U.S. 1011, 121 S.Ct. 566, 148 L.Ed.2d 485 (2000); *Haymond v. Haymond*, 2001 WL 74630, at *2 (E.D.Pa. Jan.29, 2001) (dismissal of underlying tort claim effectively dismissed the civil conspiracy claim), *aff'd sub nom.*, *Lundy v. Hochberg*, 79 Fed.Appx. 503 (3d Cir.2003); *Kist*, 2007 WL 240472, at *9 ("It should also be noted that in Pennsylvania, a claim for civil conspiracy cannot be pleaded without alleging an underlying tort.") Moreover, in order to survive any subsequent motion for

Ideal Aerosmith, Inc. v. Acutronic USA, Inc., Not Reported in F.Supp.2d (2007)

87 U.S.P.Q.2d 1341

summary judgment, Plaintiff is going to have to set forth facts substantiating its allegations of agreement and overt acts on the part of the Swiss Defendants. I also note that Plaintiff has alleged a close corporate relationship among the Defendants. Under Pennsylvania law, conspiracy requires a plurality of actors. *See Commonwealth of PA v. BASF Corp.*, 2001 WL 1807788, at *17 (Pa.Comm.Pl. Mar. 15, 2001). If the evidence demonstrates that the Defendants are merely corporate alter egos, they cannot be capable of conspiracy. *See id.*; *Academy Plaza L.L.C. v. Bryant Asset Mgmt.*, 2006 WL 1652687, at *14 (Pa. Comm. Pl. June 9, 2006) (dismissing conspiracy claim where one defendant "was so involved with the remaining defendants that they were not able to conspire").

*11 Accordingly, I deny Defendants' motions to dismiss Count 7 of the Complaint.

CONCLUSION

For the reasons set forth above, I grant Defendants' motions to dismiss Counts 1, 2, 4, 5 and 6 of the Complaint. I deny Defendants' Motions to Dismiss Counts 3, 7 and 8 of the Complaint.

Footnotes

- ¹ Defendants assert that Acutronic Group is merely a Swiss accounting designation and does not exist as a juristic entity. No proof of service has been filed by Plaintiff with respect to Acutronic Group. Nevertheless, to the extent that Acutronic Group represents any member of the "Acutronic family," it has joined in the motion to dismiss. *See* Motion by Acutronic Schweiz AG, Jung Technologies Holding AG and Thomas W. Jung to Dismiss Complaint Under Rule 12(b)(6), F.R. Civ. P. [Docket No. 11].
- ² For the same reason, Plaintiff may be unable to demonstrate that any "interception" of the Ideal Emails was intentional, as required by the Act. *See In re Pharmatrak, Inc.*, 329 F.3d 9, 23 (1st Cir.2003) ("inadvertent interceptions are not a basis for criminal or civil liability"). It bears repeating that Plaintiff has alleged that the Ideal Emails were mistakenly *sent to* Carco/Acutronic by Plaintiff and third parties.
- ³ Similarly, section 757 of the Restatement of Torts provides that "[o]ne who discloses or uses another's trade secret, without a privilege to do so, is liable to the other if ... (d) he learned the secret with notice of the facts that it was a secret and that its disclosure was made to him by mistake."

ORDER OF COURT

AND NOW, this 13th day of December, 2007, after careful consideration, and for the reasons set forth in the accompanying Opinion, the Motions to dismiss (Docket Nos. [5] and [11]) are granted with respect to Counts 1, 2, 4, 5 and 6 of the Complaint and denied with respect to Counts 3, 7 and 8 of the Complaint.

Defendants are Ordered to answer the Complaint within ten (10) days of the date of this Order.

It is further Ordered that a case management conference is scheduled for Tuesday, January 8, 2008, at 9:30 A.M. before the undersigned on the Third Floor, Suite 3280 of the U.S. Post Office and Courthouse. Counsel shall have settlement authority and parties are to be available by telephone. Position letters are to be faxed to Chief Judge Ambrose three (3) days prior to the conference.

All Citations

Not Reported in F.Supp.2d, 2007 WL 4394447, 87 U.S.P.Q.2d 1341

Ideal Aerosmith, Inc. v. Acutronic USA, Inc., Not Reported in F.Supp.2d (2007)

87 U.S.P.Q.2d 1341

International Academy of Business and Financial..., Not Reported in...

2013 WL 212640

Only the Westlaw citation is currently available.
United States District Court,
D. Colorado.

INTERNATIONAL ACADEMY OF BUSINESS
AND FINANCIAL MANAGEMENT, LIMITED,
Brett King, and Geoffrey Baring, Plaintiffs,

v.

George S. MENTZ, and American Academy of
Financial Management, LLC, Defendants.

Civil Action No. 12-cv-00463-CMA-BNB. | Jan.
18, 2013.

Attorneys and Law Firms

John Joseph Higson, Kristen Lee Repyneck, Dilworth
Paxson LLP, Philadelphia, PA, Robert Vaughan Cornish,
Jr., Dilworth Paxson LLP, Washington, DC, for Plaintiffs.

Richard W. Hanes, Hanes & Bartels, LLC, Colorado
Springs, CO, for Defendants.

ORDER GRANTING IN PART AND DENYING IN PART PLAINTIFFS' MOTION TO DISMISS COUNTERCLAIMS

CHRISTINE M. ARGUELLO, District Judge.

*1 This matter is before the Court on Plaintiffs International Academy of Business and Financial Management ("IABFM"), Brett King, and Geoffrey Baring's (collectively, "Plaintiffs") Motion to Dismiss Defendants' Counterclaims, filed on May 14, 2012. (Doc. # 20.) Jurisdiction is proper under 28 U.S.C. § 1332 (diversity jurisdiction).

I. BACKGROUND¹

Defendant George Mentz ("Mentz") is the founder and Chairman of Defendant American Academy of Financial Management, LLC ("AAFM") (collectively, "Defendants"). (Doc. # 14, ¶ 3.) AAFM is a United States entity and professional society with more than 50,000 members, associates and affiliates in over 150 countries. (*Id.*, ¶ 4.) Among other things, AAFM is engaged in the business of developing professional development

programs, certification programs, professional designations, copyrighted training programs, evaluating educational partners, adopting relevant trademarks, certification and service marks, and promoting and sanctioning certification training. (*Id.*) AAFM and its professional development programs and certifications have been recognized in several countries around the world. (*Id.*, ¶ 8.)

Defendant Brett King ("King") was under contract as an approved training affiliate of AAFM from March 2007 until he resigned on March 4, 2009. King had served as a trainer, event coordinator, a webmaster, and teacher for official AAFM and related websites and approved certification courses since 2004. (*Id.*, ¶ 10.) From approximately 2006 until he was terminated in March of 2009, Defendant Geoffrey Baring ("Baring") served as a trainer and teacher for AAFM programs. (*Id.*, ¶ 11.) King and Baring are both citizens of the Commonwealth of Australia. (Doc. # 1, ¶¶ 2, 3.)

As a condition of his representation of AAFM, King signed a Schedule B Intellectual Property Rights document (the "Agreement"), containing acknowledgments and covenants about intellectual property belonging to AAFM, promises with respect to fees owed to Mentz and AAFM, the conditional use of AAFM and related intellectual property marks, service marks, and designations, and the non-disclosure of AAFM's confidential and trade secret information and data. (*Id.*, ¶ 12; Doc. # 14-1.) Baring also "acknowledged and confessed to such agreement." (*Id.*, ¶ 12.)

King and Baring had access to all of AAFM's intellectual property during their employment. (*Id.*, ¶ 14.) Following their employment with AAFM, King and Baring formed IABFM. (*Id.*, ¶ 13.) IABFM is a non-profit worldwide professional society of financial practitioners. (Doc. # 1, ¶ 9.) IABFM is an entity of Hong Kong and has its principal place of business in Hong Kong. (*Id.*, ¶¶ 1, 10.) Although Defendants include no relevant facts about IABFM's sphere of business, Defendants have not disputed Plaintiffs' allegation that "IABFM does not offer services or membership in the United States" and that "IABFM's more than 200,000 members and affiliates are located in 145 countries throughout the world, but not including the United States." (*Id.*, ¶¶ 17, 19.) According to Defendants, King and Baring converted the intellectual property of AAFM and Mentz to their own use and benefit, (*id.* at ¶ 15), counterfeited AAFM and Mentz's property and sold it to AAFM and/or Mentz's customers for financial benefit (*id.*, ¶ 16), orchestrated a campaign of fraud to engage in identity theft and intercept customer

funds of the AAFM (*id.*, ¶ 17), and published false and defamatory emails about AAFM and Mentz. (*Id.*, ¶ 18.)

*2 Plaintiffs initiated this civil action on February 23, 2012, bringing state law tort claims for business disparagement, tortious interference with prospective business advantage, defamation, and tortious interference with prospective business advantage. (Doc. # 1, ¶¶ 82–139.) Defendants answered on April 19, 2012, and brought twelve counterclaims for: (1) breach of contract; (2) defamation; (3) service mark infringement; (4) violation of Colorado Consumer Protection Act; (5) copyright infringement; (6) civil theft; (7) civil conspiracy; (8) intentional interference with contractual relationships; (9) misappropriation of confidential information and trade secrets; (10) violation of the Computer Fraud and Abuse Act; (11) violated of the Electronic Communications Privacy Act; and (12) Application for Injunctive Relief. (Doc. # 14 at 6–23.) All counterclaims are brought by both Defendants against all three Plaintiffs.

Plaintiffs moved to dismiss Defendants' counterclaims on May 14, 2012. (Doc. # 20.) Defendants responded on June 21, 2012, thirty-eight days after the instant Motion was filed,² and Plaintiffs replied on June 29, 2012. (Doc. # 24, 25.)

II. STANDARD OF REVIEW

Plaintiffs bring the instant motion to dismiss under both Fed.R.Civ.P. 12(b)(1) and 12(b)(6). Thus, the Court will set forth the proper standard of review for motions under each rule.

A. RULE 12(b)(1)

Dismissal pursuant to Federal Rule of Civil Procedure 12(b)(1) is appropriate when the Court lacks subject matter jurisdiction over the claims asserted in the operative pleading. As set forth by the Tenth Circuit in *Holt v. United States*, 46 F.3d 1000, 1002–03 (10th Cir.1995), the standard of review for a Rule 12(b)(1) motion is as follows:

Generally, Rule 12(b)(1) motions to dismiss for lack of subject matter jurisdiction take two forms. First, a facial attack on the complaint's allegations as to subject matter jurisdiction questions the sufficiency of the complaint. In reviewing a facial attack on the

complaint, a district court must accept the allegations in the complaint as true.

Second, a party may go beyond allegations contained in the complaint and challenge the facts upon which subject matter jurisdiction depends. When reviewing a factual attack on subject matter jurisdiction, a district court may not presume the truthfulness of the complaint's factual allegations. A court has wide discretion to allow affidavits, other documents, and a limited evidentiary hearing to resolve disputed jurisdictional facts under Rule 12(b)(1). In such instances, a court's reference to evidence outside the pleadings does not convert the motion to a Rule 56 motion.

Holt v. United States, 46 F.3d 1000, 1002–03 (10th Cir.1995) (internal citations removed).

Further, the burden of establishing subject matter jurisdiction rests on the party asserting jurisdiction. See *Montoya v. Chao*, 296 F.3d 952, 955 (10th Cir.2002).

B. RULE 12(b)(6)

*3 The purpose of a motion to dismiss under Fed.R.Civ.P. 12(b)(6) for failure to state a claim is to test "the sufficiency of the allegations within the four corners of the complaint." *Mobley v. McCormick*, 40 F.3d 337, 340 (10th Cir.1994). A complaint will survive such a motion only if it contains "enough facts to state a claim to relief that is plausible on its face." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). For a motion to dismiss, "[t]he question is whether, if the allegations are true, it is plausible and not merely possible that the plaintiff is entitled to relief under the relevant law." *Christy Sports, LLC v. Deer Valley Resort Co., Ltd.*, 555 F.3d 1188, 1192 (10th Cir.2009). "The plausibility standard is not akin to a probability requirement, but it asks for more than a sheer possibility that a defendant has acted unlawfully." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quotation marks and citation omitted).

In reviewing a Rule 12(b)(6) motion, a court must accept all the well-pleaded allegations of the complaint as true and must construe them in the light most favorable to the plaintiff. *Williams v. Meese*, 926 F.2d 994, 997 (10th Cir.1991). Nevertheless, a complaint does not "suffice if it tenders 'naked assertion[s]' devoid of 'further factual enhancement.'" *Iqbal*, 556 U.S. at 678 (quoting *Twombly*, 550 U.S. at 557). "The court's function on a Rule 12(b)(6) motion is not to weigh potential evidence that the parties might present at trial, but to assess whether the plaintiff's complaint alone is legally

International Academy of Business and Financial..., Not Reported in...

sufficient to state a claim for which relief may be granted.” *Miller v. Glanz*, 948 F.2d 1562, 1565 (10th Cir.1991).

III. ANALYSIS

In this Motion, Plaintiffs have moved to dismiss all twelve counterclaims. The Court will consider each counterclaim in turn.

A. FIRST COUNTERCLAIM—BREACH OF CONTRACT

In their First Counterclaim, Defendants allege that King entered into the Agreement with Mentz and AAFM on or about March of 2007, and that Baring accepted the Agreement as binding on him. (Doc. # 14, ¶¶ 20, 21.) Defendants allege that King and Baring breached the Agreement by taking, stealing, and converting AAFM’s intellectual property, and disclosing confidential and trade secret information of AAFM. Further, Defendants allege that King and Baring breached the Agreement by failing to pay contractual fees and return property belonging to AAFM. (*Id.*, ¶ 23.)

In their motion to dismiss, Plaintiffs do not appear to challenge the sufficiency of Defendants’ allegations for this counterclaim as against King and Baring, and the Court finds that Defendants’ allegations are sufficient to state a counterclaim for breach of contract against those plaintiffs. However, Plaintiffs correctly observe that the First Counterclaim does not allege any conduct by IABFM. Thus, IABFM is dismissed as a counterclaim-defendant for the First Counterclaim.³

B. SECOND COUNTERCLAIM—DEFAMATION

*4 In their Second Counterclaim, Defendants have alleged three discrete instances of defamation by Plaintiffs. (Doc. # 14, ¶¶ 28, 30, 31.) The defamatory statements allegedly occurred on August 16, 2011, May 21, 2009, and March 23, 2009.⁴ (*See id.*) The Court will treat these as three separate counterclaims.

1. August 16, 2011 Statement

“In Colorado, the elements of a cause of action for defamation are: (1) a defamatory statement concerning another; (2) published to a third party; (3) with fault

amounting to at least negligence on the part of the publisher; and (4) either actionability of the statement irrespective of special or the existence of special damages to the plaintiff caused by the publication.” *McIntyre v. Jones*, 194 P.3d 519, 523–24 (Colo.App.2008) (quoting *Williams v. Dist. Court*, 866 P.2d 908, 911 n. 4 (Colo.1993)). Upon review of the allegations, the Court finds that the August 16, 2011 statement is sufficient to form the basis for a counterclaim for defamation.⁵ (*See* Doc. # 14, ¶ 28.)

2. May 21, 2009 and March 23, 2009 Statements

Plaintiffs contend that any counterclaims for defamation based on the May 21, 2009 or the March 23, 2009 statements are time-barred. (Doc. # 20 at 5.) The Court agrees. Under Colorado law, there is a one-year statute of limitations for defamation claims. *See* Colo.Rev.Stat. § 13–80–103(a). The cause of action “accrues when the defamatory statements are published.” *See Conrad v. The Educ. Res. Inst.*, 652 F.Supp.2d 1172, 1186 (D.Colo.2009) (citing *Russell v. McMillen*, 685 P.2d 255, 258 (Colo.App.1984)). Thus, any counterclaims for defamation based on the May 21, 2009 and March 23, 2009 statements are time-barred because they were published more than one year before this case commenced.

Defendants’ only response to Plaintiffs’ statute of limitations argument is their puzzling assertion that such an argument is “misplaced in a motion to dismiss under Rule 12(b)(6).” (Doc. # 24 at 4.) Defendants fail to support this assertion with any authority, and courts routinely decide issues relating to statutes of limitations on motions to dismiss. *See, e.g., Jackson v. Standifird*, 463 F. App’x 736, 737 (10th Cir.2012) (“Dismissal of a claim as time-barred is treated as a dismissal for failure to state a claim”); *Yoder v. Honeywell Inc.*, 104 F.3d 1215, 1224 (10th Cir.1997) (applying *de novo* review to district court’s dismissal for failure to state a claim on the grounds that the claim was time-barred). Thus, the Court will dismiss with prejudice Defendants’ counterclaims for defamation based on the May 21, 2009 and the March 23, 2009 statements because they are time-barred. *See Womble v. Salt Lake City Corp.*, 84 F. App’x 18, 20–21 (10th Cir.2003) (dismissal of claim as time-barred should be with prejudice).

C. THIRD COUNTERCLAIM—SERVICE MARK INFRINGEMENT (LANHAM ACT)

In their Third Counterclaim, Defendants allege that Plaintiffs’ “use and sale” of their marks constitute

International Academy of Business and Financial..., Not Reported in...

trademark infringement under Section 32 of the Lanham Act, 15 U.S.C. § 1114, and unfair competition under Section 43(a) of the Lanham Act, 15 U.S.C. § 1125(a). (Doc. # 14, ¶¶ 51–52.) Plaintiffs assert that the Court lacks subject matter jurisdiction over this counterclaim.

*5 The Lanham Act “confers broad jurisdictional powers upon the courts of the United States.” *Steele v. Bulova Watch Co.*, 344 U.S. 280, 283 (1952). Thus, Congress has the power to regulate foreign trade practices of United States citizens, even when some of the acts occur outside the territorial boundaries of the United States. *See id.* at 285–86. In this case, however, it is undisputed that none of the Plaintiffs are citizens of the United States. (Doc. # 1, ¶¶ 1–3; Doc. # 14, ¶ 2.) Because none of the Plaintiffs are citizens of the United States, the Court must determine whether it has subject matter jurisdiction over this counterclaim. *See McBee v. Delica Co., Ltd.*, 417 F.3d 107, 117 (1st Cir.2005) (finding that most courts treat the extraterritoriality application of the Lanham Act as an issue relating to subject matter jurisdiction).

Although *Bulova Watch* made clear that the Lanham Act has some extraterritorial application, the Supreme Court has not laid down a precise test for when a district court may exercise extraterritorial jurisdiction over a foreign infringer. *See McBee*, 417 F.3d at 117. The circuit courts, however, have formulated a variety of tests for determining when extraterritorial application of the Lanham Act is appropriate.⁶ *See id.* (listing different tests). The most commonly employed test appears to be the one set forth by the Second Circuit in *Vanity Fair Mills, Inc. v. T. Eaton Co.*, 234 F.2d 633 (2d Cir.1956). *Vanity Fair* stresses three factors: (1) whether the defendant’s conduct has had a substantial effect on United States commerce; (2) whether the defendant is a United States citizen; and (3) whether there is conflict with trademark rights established under foreign law. *See id.* at 642; *see also Int’l Café, S.A.L., v. Hard Rock Café Int’l (U.S.A.), Inc.*, 252 F.3d 1274, 1278–79 (11th Cir.2001) (applying *Vanity Fair*); *Nintendo of Am., Inc., v. Aeropower Co., Ltd.*, 34 F.3d 246, 250–51 (4th Cir.1994) (adopting *Vanity Fair*, although requiring a “significant” rather than a “substantial” effect); *but see Star-Kist Foods, Inc. v. P.J. Rhodes & Co.*, 769 F.2d 1393 (9th Cir.1985) (plaintiff must show (1) some effect on United States commerce, (2) the effect must be sufficiently great to present a cognizable injury to plaintiff, and (3) the interests and links to American commerce must be sufficiently strong in relation to those of other nations); *McBee*, 417 F.3d 107 at 120 (holding that the Lanham Act grants subject matter jurisdiction over extraterritorial conduct “only where the conduct has a substantial effect on United States commerce.”). Although these tests vary slightly, they share the commonality that extraterritorial

application of the Lanham Act is only proper when a party shows that the infringing activity has a substantial or significant effect on United States commerce. *See Basis Int’l Ltd., v. Research in Motion Ltd.*, 827 F.Supp.2d 1302, 1306 (D.N.M.2011).

*6 Upon review of Defendants’ Third Counterclaim, the Court finds that Defendants have not alleged that Plaintiffs’ infringing activities had any effect on United States commerce, let alone a substantial or significant one. Defendants do not dispute that Plaintiffs are not United States citizens, nor do they offer any allegations that Plaintiffs have used Defendants’ marks in connection with any United States commerce. Given the absence of allegations showing that Plaintiffs’ conduct had a substantial or significant effect on United States commerce, this Court lacks jurisdiction over Defendants’ Third Counterclaim. *See Love v. The Mail on Sunday*, 473 F.Supp.2d 1052, 1056 (C.D.Cal.2007) (Lanham Act does not apply where there is no evidence that infringing activity by foreign defendants affected United States commerce).

Defendants make two wholly unpersuasive arguments in their Response. First, Defendants contend that Plaintiffs’ argument regarding subject matter jurisdiction is a “bizarre anomaly” because Plaintiffs originally invoked this Court’s jurisdiction by initiating this civil action. (Doc. # 24 at 4.) However, the fact that the Court may properly exercise personal jurisdiction over Plaintiffs and subject matter jurisdiction over some claims does not necessarily mean that the Court possesses subject matter jurisdiction over all claims. Second, Defendants note that the “publications in which Plaintiffs’ [*sic*] infringe Defendants’ registered service marks appear on the internet which is available to viewers and users in the United States.” (*Id.*) Although not framed as an argument per se, Defendants seem to be suggesting that this Court possesses jurisdiction over extraterritorial trademark infringement by foreign defendants simply because a website is accessible in the United States. Not surprisingly, Defendants cite no authority for this sweeping proposition. The allegation that a website is accessible in the United States does not necessarily demonstrate that the allegedly infringing conduct has a substantial or significant effect on United States commerce. *See Gallup, Inc. v. Bus. Research Bureau (Pvt.) Ltd.*, 688 F.Supp.2d 915, 925 (N.D. Cal.2010) (rejecting similar argument as “insufficient, unpersuasive, and unfair”). Defendants do not dispute that Plaintiffs do not offer services or membership in the United States, nor do they allege that Plaintiffs’ conduct has had any impact on United States commerce. Thus, the Court dismisses Defendants’ Third Counterclaim for lack of subject matter jurisdiction.

International Academy of Business and Financial..., Not Reported in...

D. FOURTH COUNTERCLAIM—VIOLATION OF COLORADO CONSUMER PROTECTION ACT

In their Fourth Counterclaim, Defendants allege that Plaintiffs violated the Colorado Consumer Protection Act (“CCPA”), C.R.S. § 6–1–105(a), (b), and (c). The CCPA was enacted to regulate commercial activities that “because of their nature, may prove injurious, offensive, or dangerous to the public.” *Rhino Linings USA, Inc. v. Rocky Mountain Rhino Lining, Inc.*, 62 P.3d 142, 146 (Colo.2003) (citation omitted). The elements to bring a private cause of action under the CCPA are: “(1) that the defendant engaged in an unfair or deceptive trade practice; (2) that the challenged practice occurred in the course of defendant’s business, vocation, or occupation; (3) that it significantly impacts the public as actual or potential consumers of the defendant’s goods, services, or property; (4) that the plaintiff suffered injury in fact to a legally protected interest; and (5) that the challenged practice caused the plaintiff’s injury. *Id.* at 146–47. Such a claim must be pled with particularity under Fed.R.Civ.P. 9(b). *Gates Corp. v. Dorman Prods., Inc.*, No. 09–cv–02058, 2009 WL 5126556, at *5 (D.Colo. Dec. 18, 2009) (unpublished). Rule 9(b) provides that “[i]n all averments of fraud or mistake, the circumstances constituting fraud or mistake shall be stated with particularity.” Thus, a party claiming fraud must “set forth the time, place and contents of the false representation, the identity of the party making the false statements and the consequences thereof.” *Koch v. Koch Indus., Inc.*, 203 F.3d 1202, 1236 (10th Cir.2000); *see also U.S. ex rel. Lemmon v. Envirocare of Utah, Inc.*, 614 F.3d 1163, 1172 (10th Cir.2010) (the purpose of Rule 9(b) is to afford the defendant fair notice of plaintiff’s claims and the factual grounds upon which they are based).

*7 Defendants’ Fourth Counterclaim is woefully inadequate under the *Koch* standard. Defendants simply allege that the Plaintiffs’ “acts and transactions set forth above constitute deceptive trade practices.” (Doc. # 14, ¶ 58.) This allegation does not identify any particular conduct by Plaintiffs, how such conduct was “unfair or deceptive,” or where and when such conduct occurred. *See Hansen v. Auto–Owners Ins. Co.*, No. 09–cv–02736, 2010 WL 749820, at *3 (D.Colo. Mar. 4, 2010) (unpublished) (dismissing CCPA claim because the plaintiff failed to identify the allegedly misleading representations). Moreover, Defendants do not allege that any such deceptive trade practices had a significant impact on the public.*

Defendants argue in their Response that their Fourth Counterclaim is sufficient because it “recites the

particular statutory provisions alleged to have been violated.” (Doc. # 14 at 5.) However, the mere invocation of a statute is not sufficient to state a claim upon which relief may be granted. *See Lemmon*, 614 F.3d at 1172; *Iqbal*, 556 U.S. at 678 (“Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice.”). Defendants also assert that their Fourth Counterclaim is sufficient because it “makes reference to previous paragraphs of the counterclaim.” (Doc. # 14 at 5.) This Court has strongly criticized such use of “shotgun pleading,” by which a party pleads several counts or causes of action, each of which incorporates by reference the entirety of its predecessors.* *Jacobs v. Credit Suisse First Boston*, No. 11–cv–00042, 2011 WL 4537007, at *6 (D.Colo. Sept. 30, 2011) (unpublished) (finding “shotgun pleading” to be a “defect” contributing to an award of sanctions). As this Court noted, “the shotgun pleader foists off one of the pleading lawyer’s critical tasks—sifting a mountain of facts down to a handful of those that are relevant to a given claim—onto the reader.” *Id.* Courts roundly decry shotgun pleading as a subject of “great dismay,” “intolerable,” and “in a very real sense ... [an] obstruction of justice.” *Strategic Income Fund, L.L.C. v. Spear, Leeds & Kellogg Corp.*, 305 F.3d 1293, 1295–96 n. 9, 10 (11th Cir.2002). The Court will not act as counsel for Defendants and attempt to determine which facts may support this Fourth Counterclaim. Defendants have not made even a cursory attempt to specify what conduct by Plaintiffs violated the CCPA; thus, the Court will dismiss Defendants’ Fourth Counterclaim for failure to state a claim.

E. FIFTH COUNTERCLAIM—COPYRIGHT INFRINGEMENT

In their Fifth Counterclaim, Defendants allege that Plaintiffs violated the United States Copyright Act, 17 U.S.C. § 101, *et seq.* As with Defendants’ Lanham Act Counterclaim, this Fifth Counterclaim concerns only extraterritorial conduct by Plaintiffs. “It is well established that copyright laws generally do not have extraterritorial application.”* *Predator Int’l Inc., v. Gamo Outdoor USA, Inc.*, 863 F.Supp.2d 1055, 1065 (D.Colo.2012) (quoting *Update Art, Inc. v. Modiin Pub., Ltd.*, 843 F.2d 67, 73 (2d Cir.1988)); *see also Subafilms, Ltd. v. MGM–Pathe Commc’ns Co.*, 24 F.3d 1088, 1099 (9th Cir.1994) (“the mere authorization of acts of infringement that are not cognizable under the United States copyright laws because they occur entirely outside of the United States does not state a claim for infringement under the Copyright Act.”).

International Academy of Business and Financial..., Not Reported in...

*8 The extraterritorial application of the Copyright Act represents an element of a claim and does not affect subject matter jurisdiction. *See Wood v. Houghton Mifflin Harcourt Pub. Co.*, 569 F.Supp.2d 1135, 1138 (D.Colo.2008); *Litecubes, LLC v. N. Light Prods., Inc.*, 523 F.3d 1353, 1368 (Fed.Cir.2008) (holding that extraterritorial application of the Copyright Act “is properly treated as an element of the claim which must be proven before relief can be granted, not a question of subject matter jurisdiction”). Because Defendants’ Fifth Counterclaim appears to concern only extraterritorial conduct,¹⁰ Defendants have failed to plead a necessary element of a copyright infringement claim, and therefore the Court will dismiss Defendants’ Fifth Counterclaim for failure to state a claim upon which relief may be granted.

F. SIXTH COUNTERCLAIM—CIVIL THEFT

In their Sixth Counterclaim, Defendants have alleged that Plaintiffs violated C.R.S. § 18–4–405 by “knowingly obtain[ing] control over intellectual and personal property of AAFM and Mentz without their authorization, including web sites, data, member accounts, networking accounts, organizational technology and domain names.” (Doc. # 14, ¶¶ 70–71.) Section 18–4–405 provides that “the owner [of property obtained by theft, robbery, or burglary] may maintain an action not only against the taker thereof but also against any person in whose possession he finds the property.” Thus, to plead a claim for civil theft, Defendants must plead facts showing that Plaintiffs obtained control over Defendants property in circumstances amounting to theft, robbery, or burglary. *Martinez v. Nash Finch Co.*, 886 F.Supp.2d 1212, 2012 WL 3307000, at *7 (D.Colo.2012). Defendants have provided no factual allegations to support this claim; rather, Defendants have merely cited to a statute and recited the elements of a claim under that statute. (Doc. # 14, ¶¶ 69–74.) Formulaic recitations of the elements of a cause of action do not suffice to state a claim. *See Iqbal*, 556 U.S. at 678–79. Thus, the Court will dismiss Defendants’ Sixth Counterclaim for failure to state a claim upon which relief may be granted.

G. SEVENTH COUNTERCLAIM—CIVIL CONSPIRACY

In their Seventh Counterclaim, Defendants have brought a claim for civil conspiracy, alleging that King and Baring agreed to “accomplish the unlawful goals described in paragraphs 1–69 and one or more acts were performed to accomplish the unlawful goals.” (Doc. # 14, ¶ 76.) Defendants also allege that King and Baring agreed to

“accomplish the goals” through “unlawful means” and “unlawful acts.”

Defendants’ allegations merely recite the elements of a civil conspiracy claim,¹¹ and provide no factual allegations to support the claim. As such, the Court will dismiss Defendants’ Seventh Counterclaim for failure to state a claim upon which relief may be granted.

H. EIGHTH COUNTERCLAIM—INTENTIONAL INTERFERENCE WITH CONTRACTUAL RELATIONSHIPS

*9 In their Eighth Counterclaim, Defendants have alleged that Plaintiffs interfered with a contract between Mentz and AAFM and “Mr. Carl Thong and Mr. ‘Meocre’ Li Kwok Wing.” (Doc. # 14, ¶ 80 .) Although this Counterclaim contains more factual allegations than most of the other counterclaims, Defendants have not alleged that Plaintiffs had knowledge of the contractual relationship between Mentz/AAFM and Thong/Wing. In order to intentionally interfere with a contract, Plaintiffs must have been aware of the contractual relationship. *See Krystkowiak v. W.O. Brisben Cos., Inc.*, 90 P.3d 859, 871 (Colo.2004) (“To be liable for intentional interference with contract, a defendant must 1) be aware of a contract between two parties, 2) intend that one of the parties breach the contract, 3) and induce the party to breach or make it impossible for the party to perform the contract.”). As there are no allegations that Plaintiffs were aware of a contract between Mentz/AAFM and Thong/Wing, Defendants’ Eighth Counterclaim is dismissed for failure to state a claim upon which relief may be granted.

I. NINTH COUNTERCLAIM—MISAPPROPRIATION OF A TRADE SECRET

In their Ninth Counterclaim, Defendants allege that Plaintiffs “took AAFM’s confidential and trade secret information without AAFM’s authorization,” and that Plaintiffs are now using that information to compete against AAFM. (Doc. # 14, ¶ 91.) Defendants conclusorily assert that AAFM’s “trading information meets the definition of trade secrets” under Colorado law. (*Id.*, ¶ 93.) The Colorado Uniform Trade Secrets Act (“UTSA”) defines a trade secret as:

[T]he whole or any portion or phase of any scientific or technical information, design, process, formula, improvement, confidential business or financial information,

International Academy of Business and Financial..., Not Reported in...

listing of names, addresses, or telephone numbers, or other information relating to any business or profession which is secret and of value.

C.R.S. § 7–74–102(4). A party alleging misappropriation of a trade secret must produce evidence “of the specific types of confidential information ... with sufficient particularity to identify the existence of its claimed trade secrets.” *Saturn Sys., Inc. v. Militare*, 252 P.2d 516, 522 (Colo.App.2011). Although Defendants assert that its “trading information” satisfies the definition of “trade secrets” under the UTSA, Defendants neglect to define the term “trading information” or otherwise explain which particular trade secrets are alleged to have been misappropriated. The Court does not accept as true “legal conclusions” that are unsupported by any factual allegations. *See Iqbal*, 556 U.S. at 678. Thus, Defendants have not pleaded sufficient facts to show that the information allegedly misappropriated by Plaintiffs satisfies the definition of a “trade secret” under the UTSA. Thus, Defendants’ Ninth Counterclaim is dismissed for failure to state a claim upon which relief may be granted.

J. TENTH COUNTERCLAIM—VIOLATION OF THE COMPUTER FRAUD AND ABUSE ACT

*10 In their Tenth Counterclaim, Defendants allege that Plaintiffs violated the Computer Fraud and Abuse Act (“CFAA”), 18 U.S.C. § 1030(a)(4), which provides that “whoever knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, shall have violated the Act.”

The elements of a civil claim premised on § 1030(a)(4) are: (i) the defendant accessed a protected computer, (ii) the access was either unauthorized or beyond the scope of access for which the person was authorized, (iii) the defendant accessed the computer with an intent to defraud and in furtherance of a scheme to defraud, and (iv) the defendant “obtained anything of value” as a result. *Triad Consultants, Inc. v. Wiggins*, 249 F. App’x 38, 40 (10th Cir.2007). In addition, § 1030(g) imposes an additional element before civil liability may lie—that the defendant “suffers damage or loss by reason of a violation of this section.”

Defendants again fail to comply with federal pleading standards because they simply recite the elements of a claim without any supporting factual allegations. (*See*

Doc. # 14, ¶ 102) (alleging that Plaintiffs’ “knowingly and with intent to defraud, accessed AAFM’s protected computer systems, without authorization and/or in excess of authorized access.”). Another deficiency is that Defendants have failed to allege that they suffered any loss from Plaintiffs’ alleged unauthorized access of their computer systems; rather, Defendants assert that the value of Plaintiffs’ use was more than \$5,000.00. (*Id.*, ¶ 103.) Value gained by Plaintiffs is not the equivalent of loss suffered by Defendants. *See* 18 U.S.C. § 1030(e)(11) (defining the term “loss” as “any reasonable cost to any victim”) (emphasis added). Thus, a “loss” exists “where the victim of the unauthorized access incurs particular charges or expenses as a result of the unauthorized access.” *Am. Family Mut. Ins. Co. v. Gustafson*, No. 08–cv–02772, 2011 WL 782574, at *4 (D.Colo. Feb. 25, 2011) (unpublished). No such allegations of “loss” are provided by Defendants; thus, the Court dismisses Defendants’ Tenth Counterclaim for failure to state a claim upon which relief may be granted.

K. ELEVENTH COUNTERCLAIM—VIOLATION OF ELECTRONIC COMMUNICATIONS PRIVACY ACT

In their Eleventh Counterclaim, Defendants allege that Plaintiffs violated the Electronic Communications Privacy Act (“ECPA”), 18 U.S.C. § 2701(a), which makes it an offense to “(1) intentionally access[] without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceed[] an authorization to access that facility; and thereby obtain[], alter[], or prevent[] authorized access to a wire or electronic communication while it is in electronic storage in such system.” Once again, Defendants allege that Plaintiffs violated this statute without providing sufficient factual allegations. (Doc. # 14, ¶ 106) (alleging only that Plaintiffs “intentionally and willfully accessed AAFM’s stored electronic communications without authorization”). Thus, Defendants’ Eleventh Counterclaim is dismissed for failure to state a claim upon which relief may be granted.

L. TWELFTH COUNTERCLAIM—APPLICATION FOR INJUNCTIVE RELIEF

*11 In this Twelfth “Counterclaim,” Defendants seek injunctive relief in the form of a preliminary injunction and, after trial, a permanent injunction.¹² (Doc. # 14, ¶¶ 110, 111.) However, no motion is presently before the Court and so the Court will not address whether a preliminary injunction is warranted on the claims that have not been dismissed. Further, at this stage of the case,

International Academy of Business and Financial..., Not Reported in...

the Court cannot determine whether a permanent injunction will be necessary. Thus, the Court will deny Plaintiffs' motion to dismiss Defendants' Twelfth "Counterclaim" without prejudice as it is not yet ripe for consideration.

IV. CONCLUSION

Based on the foregoing, it is ORDERED that Plaintiffs' Motion to Dismiss Defendants' Counterclaims (Doc. # 20) is GRANTED IN PART and DENIED IN PART. Specifically, it is ORDERED that:

(1) Defendants' First Counterclaim is DISMISSED against Plaintiff IABFM for failure to state a claim under Fed.R.Civ.P. 12(b)(6). The First Counterclaim remains against Defendants King and Baring;

(2) Defendants' Second Counterclaim is DISMISSED WITH PREJUDICE insofar as it alleges defamation based on the March 21, 2009 and March 23, 2009 statements

allegedly made by Plaintiffs. The Second Counterclaim remains insofar as it alleges defamation based on the August 16, 2011 statement allegedly made by Plaintiffs;

(3) Defendants' Third Counterclaim is DISMISSED for lack of subject matter jurisdiction under Fed.R.Civ.P. 12(b)(1);

(4) Defendants' Fourth, Fifth, Sixth, Seventh, Eighth, Ninth, Tenth, and Eleventh Counterclaims are DISMISSED for failure to state a claim under Fed.R.Civ.P. 12(b)(6); and

(5) Defendants have thirty (30) days to file amended Counterclaims, should they wish to do so.

All Citations

Not Reported in F.Supp.2d, 2013 WL 212640

Footnotes

- ¹ Unless otherwise noted, the following facts are allegations taken from the "counterclaims" section of Defendants' Answer and are deemed true for purposes of the instant motion. (See Doc. # 14 at 6–23.) When the Court refers to a specific paragraph in the Answer, the Court is referring to the paragraphs in the counterclaims portion of the Answer.
- ² In their Reply, Plaintiffs request that the Court strike Defendants' Response as untimely. (Doc. # 25 at 1–2.) The Local Rules for the District of Colorado provide that "[t]he responding party shall have 21 days after the date of service of a motion, or such lesser or greater time as the court may allow, in which to file a response." D.C.COLO.LCivR 7.1.C. Thus, Defendants filed their Response well after the time for filing a response had passed. As Plaintiffs observe, Defendants have been represented by counsel at all times, never sought an extension of time to file their Response, and have provided no excuse for their untimely filing. The Court main-tains broad discretion to strike a responsive document as untimely. See *Curran v. AMI Fire-place Co., Inc.*, 163 F. App'x 714, 718 (10th Cir.2006) (district court has discretion to strike untimely response). Although the Court does not condone Defendants' tardiness, the Court finds that consideration of the Response will not change the resolution of Plaintiffs' Motion. Thus, the Court will exercise its discretion and decline to strike the Response.
- ³ The absence of any allegations of conduct by IABFM also dooms Defendants' Fourth, Fifth, and Seventh Counterclaims against IABFM. However, as discussed below, those counterclaims are dismissed against all Defendants for other reasons.
- ⁴ Defendants also raise some general allegations that King and Baring adopted pseudonyms and initiated various smear and defamation campaigns against Plaintiffs. (Doc. # 14, ¶ 32.) To the extent that Defendants sought to bring a claim for defamation regarding these statements, such allegations are vague, conclusory, and non-specific. Defendants have not set forth the words that are allegedly defamatory, nor have they provided any dates on which such statements were made. See *Walters v. Linhof*, 559 F.Supp. 1231, 1234 (D.Colo.1983). As such, Defendants have not provided sufficient factual allegations "to state a claim to relief that is plausible on its face" based on such statements. *Twombly*, 550 U.S. at 570.
- ⁵ Although Plaintiffs contend that the Second Counterclaim should be dismissed in its entirety, Plaintiffs make no argument with respect to the August 16, 2011 statement.
- ⁶ The parties did not cite to any relevant Tenth Circuit authority on this issue, and the Court has found none upon independent investigation.
- ⁷ Under Colorado law, courts consider the following factors to ascertain the public impact of a challenged practice: "(1) the number

International Academy of Business and Financial..., Not Reported in...

of consumers directly affected by the challenged practice; (2) the relative sophistication and bargaining power of the consumers affected by the challenged practice; and (3) evidence that the challenged practice has previously impacted other consumers or has significant potential to do so in the future.” *Brodeur v. Am. Home Assur. Co.*, 169 P.3d 139, 155 (Colo.2007) (citing *Rhino Linings*, 62 P.3d at 149).

8 Plaintiffs repeat this defective pleading practice throughout the counterclaims portion of their Answer.

9 An exception exists where the infringing party committed a predicate act of infringement within the United States. *Estate of Stewart v. Sugar Hill Music Pub., Ltd.*, No. 10 Civ. 2632, 2012 WL 4900927, at *5 (S.D.N.Y. Oct. 12, 2012) (unpublished). Defendants have not alleged that there was any predicate act of infringement that occurred in the United States.

10 As with their Lanham Act counterclaim, Defendants argue that the Court has jurisdiction because the alleged copyright infringements appeared on a website accessible in the United States. Defendants have not submitted any authority for this proposition, and given the absence of any allegations that the allegedly infringing conduct had any effect on United States commerce, the Court finds this allegation insufficient to provide this Court with jurisdiction.

11 To establish a civil conspiracy in Colorado, Defendants must show: “(1) two or more persons; an object to be accomplished; (3) a meeting of the minds on the object or course of action; (4) an unlawful overt act; and (5) damages as to the proximate result.” *Nelson v. Elway*, 908 P.2d 102, 106 (Colo.1995).

12 This counterclaim is a misnomer as injunctive relief “is a type of relief ... not a cause of action.” *Colo. Rail Passenger Ass’n v. Fed. Transit Admin.*, No. 09–cv–01135, 2011 WL 5184524, at *2 (D.Colo. Dec. 15, 2010) (unpublished).

End of Document

© 2015 Thomson Reuters. No claim to original U.S. Government Works.

SBM Site Services, LLC v. Garrett, Not Reported in F.Supp.2d (2012)

2012 WL 628619

Only the Westlaw citation is currently available.
United States District Court,
D. Colorado.

SBM SITE SERVICES, LLC, an Oregon limited
liability company, Plaintiff,

v.

John GARRETT, and Crown Building
Maintenance, Inc. d/b/a Able Building
Maintenance d/b/a Able Services d/b/a Able
Acquisition Corp., Defendants.

Civil No. 10-cv-00385-WJM-BNB. | Feb. 27, 2012.

Attorneys and Law Firms

Khari Jamil Tillery, Ajay Sundar Krishnan, Jeffrey Robert
Chanin, Steven Paul Ragland, Kecker & Van Nest, LLP,
San Francisco, CA, Jeffrey A. Chase, N. Reid Neureiter,
Husch Blackwell LLP, Denver, CO, for Plaintiff.

John Garrett, Windsor, CO, pro se.

Daniel M. Reilly, Kent Charles Modesitt, Larry S. Pozner,
Marisa B. Hudson-Arney, Michael Andrew Rollin, Reilly
Pozner, L.L.P., Denver, CO, Lori Ann Lutzker, Robert
Alfred Samuel Bleicher, Carr, McClellan, Ingersoll,
Thompson & Horn, P.C., Burlingame, CA, for
Defendants.

ORDER DENYING DEFENDANTS' MOTIONS TO DISMISS

WILLIAM J. MARTÍNEZ, District Judge.

*1 Plaintiff SBM Site Services ("Plaintiff" or "SBM") brings claims against John Garrett ("Garrett") and Crown Building Maintenance Inc. d/b/a Able Building Maintenance ("Able") for violation of the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, and brings as well various common law and Colorado statutory claims against these Defendants. (Am. Compl. (ECF No. 190).) Before the Court are Garrett's Partial Motion to Dismiss (ECF No. 196) and Able's Motion to Dismiss (ECF No. 217) (together the "Motions"). For the reasons set forth below, the Motions are denied.

I. LEGAL STANDARD

Both Garrett and Able bring their Motions to Dismiss at least in part under Federal Rule of Civil Procedure 12(b)(6). The purpose of a motion to dismiss pursuant to Rule 12(b)(6) is to test "the sufficiency of the allegations within the four corners of the complaint after taking those allegations as true." *Mobley v. McCormick*, 40 F.3d 337, 340 (10th Cir.1994). To survive a Rule 12(b)(6) motion, "[t]he complaint must plead sufficient facts, taken as true, to provide 'plausible grounds' that discovery will reveal evidence to support the plaintiff's allegations." *Shero v. City of Grove, Okla.*, 510 F.3d 1196, 1200 (10th Cir.2007) (citing *Bell Atl. Corp. v. Twombly*, 550 U.S. 544 (2007)). The concept of "plausibility" at the dismissal stage refers not to whether the allegations are likely to be true; the court must assume them to be true. *Christy Sports, LLC v. Deer Valley Resort Co., Ltd.*, 555 F.3d 1188, 1192-93 (10th Cir.2009). The question is whether, if the allegations are true, it is plausible and not merely possible that the plaintiff is entitled to relief under the relevant law. *Robbins v. Oklahoma*, 519 F.3d 1242, 1247 (10th Cir.2008). Overall, "[t]he court's function on a Rule 12(b)(6) motion is not to weigh potential evidence that the parties might present at trial, but to assess whether the plaintiff's complaint alone is legally sufficient to state a claim for which relief may be granted." *Sutton v. Utah State Sch. for the Deaf & Blind*, 173 F.3d 1226, 1236 (10th Cir.1999) (citation omitted).

Able also brings its Motion to Dismiss pursuant to Federal Rule of Civil Procedure 12(b)(1). The purpose of a motion to dismiss pursuant to Rule 12(b)(1) is to test whether the Court has subject-matter jurisdiction to properly hear the case before it. Dismissal of a federal claim for lack of subject-matter jurisdiction "is proper only when the claim is 'so insubstantial, implausible, foreclosed by prior decisions of this Court, or otherwise completely devoid of merit as not to involve a federal controversy.'" *Steel Co. v. Citizens for a Better Env't*, 523 U.S. 83, 89 (1998) (quoting *Oneida Indian Nation v. County of Oneida*, 414 U.S. 661, 666 (1974)). When reviewing a facial attack on a complaint pursuant to Rule 12(b)(1), as is asserted in this case, the Court also accepts the allegations of the complaint as true. *Holt v. United States*, 46 F.3d 1000, 1002 (10th Cir.1995).

II. FACTUAL BACKGROUND

SBM Site Services, LLC v. Garrett, Not Reported in F.Supp.2d (2012)

*2 The operative complaint in this case is Plaintiff's First Amended Complaint, filed January 24, 2011. (ECF No. 190.) The relevant facts, as pled in the First Amended Complaint and accepted as true for purposes of the instant Motions, are as follows.

Plaintiff SBM provides various facilities support services such as janitorial, recycling, and moving services to its customers. (Am.Compl.¶ 12.) SBM maintains a "great deal" of confidential information in an electronic database known as its "Knowledge Portal". (*Id.* ¶ 14.) The Knowledge Portal contains all of the forms and procedures necessary to operate SBM's business. (*Id.*) It also contains confidential customer lists and confidential information pertaining to particular customers. (*Id.*)

For nearly fifteen years, Defendant John Garrett was employed by SBM. (*Id.* ¶ 13.) At the time of his departure from SBM, Garrett was the Senior Vice President—Chief Business Development Officer and one of only five employees that reported directly to SBM's Chief Operating Officer. (*Id.*) SBM provided Garrett with access to the Knowledge Portal for purposes of performing the functions of his job. (*Id.* ¶ 14.)

Garrett primarily worked remotely for SBM from a home office in Windsor, Colorado. (*Id.* ¶ 16.) Because he worked remotely, SBM provided Garrett with two desktop computers and two laptop computers. (*Id.*) Garrett used these SBM-provided devices to remotely access SBM's computer system, including the Knowledge Portal. (*Id.*) SBM also provided Garrett with an external drive to maintain an archive of bids, proposals, templates, and other marketing tools. (*Id.*)

SBM's Employee Handbook provides: "No one is permitted to remove or make copies of any SBM records, reports or documents without prior management approval." (*Id.* ¶ 18.) Additionally, on February 27, 1997, Garrett executed a Confidentiality Agreement in which he agreed, in relevant part, "to hold in confidence and not disclose any Company business, including but not limited to: accounting records, employee records, customer lists and contracts, specialized training information, processes and operations ..." (*Id.* 19.) On March 27, 2006, Garrett also executed a Non-Competition, Non-Solicitation and Confidentiality Employment Agreement ("Non-Compete") in which he agreed not to "engage or participate, directly or indirectly, in any business or activity which directly or indirectly competes with or is similar to the business" of SBM for three years after termination of his employment. (*Id.* ¶ 20.)

Defendant Able is a direct competitor of SBM. (*Id.* ¶ 24.) In December 2009, Garrett had multiple conversations

with high-ranking officers at Able. (*Id.* ¶¶ 26, 28.) Shortly after one of these meetings, Garrett asked Christine Kieft, his administrative assistant, to access the Knowledge Portal and download all available files under each category. (*Id.* ¶ 26.) Garrett later asked Kieft to mail him a CD with all of these documents on it. (*Id.* ¶ 29.)

*3 On January 3, 2010, Garrett met with representatives from Able to discuss expanding Able's business services. (*Id.* ¶ 30.) In follow-up correspondence to that meeting, Able informed Garrett that he would be heading up a new division—Able Building Maintenance. (*Id.*) The following day, Garrett informally informed SBM that he was resigning effective January 22, 2010. (*Id.* ¶ 31.) SBM informed Garrett that, upon his departure from employment, he would be required to return all SBM property, including equipment, records, and confidential and/or trade secret information in any form or medium. (*Id.* ¶ 35.) Garrett confirmed that he would return the property. (*Id.*)

On January 11, 2010, Able made a written offer of employment to Garrett. (*Id.* ¶ 32.) Garrett then directed Kieft to contact members of the sales team and have them provide their most current customer contact information sheet. (*Id.*) Upon receipt of this information, Garrett e-mailed it to his personal e-mail account. (*Id.* ¶ 33.) Between January 10, 2010 and January 22, 2010, Garrett sent leads and other confidential information of SBM to executives at Able. (*Id.* ¶ 34.)

Garrett met with SBM's director of human resources on January 26, 2010 but failed to return any of his company computers or the disk with information downloaded from the Knowledge Portal that was created by Kieft. (*Id.* ¶ 38.) SBM scheduled a follow-up meeting for January 29, 2010 to collect these items but Garrett cancelled and informed SBM that all equipment had been shipped. (*Id.*)

Garrett began his employment with Able on January 28, 2010. (*Id.* ¶ 41.) SBM alleges that Garrett and Able have used and are actively using its confidential trade secret information, including customer lists, historical bid information, and preferred supplier agreements, to lure customers away from SBM. (*Id.* ¶¶ 42–43.) Garrett also loaded SBM's confidential trade secret information onto a laptop provided to him by Able. (*Id.* ¶ 44.)

SBM did not receive Garrett's laptop until February 16, 2010. (*Id.* ¶ 39.) When SBM received the laptop, it had been encrypted with a drive-lock to prevent access. (*Id.*) To date, Garrett has not provided SBM with the password to access the laptop. (*Id.*) SBM has since learned that the laptop was "intentionally erased". (*Id.*)

Based on these factual allegations, SBM brings the following claims: (1) Breach of Confidentiality Agreement against Garrett; (2) Breach of Contract—Non-Compete Agreement against Garrett; (3) Breach of Implied Duty of Good Faith and Fair Dealing against Garrett; (4) Inevitable Disclosure against Garrett and Able; (5) Misappropriation of Trade Secrets in violation of Colo.Rev.Stat. § 7-74-101 *et seq.* against Garrett and Able; (6) Civil Theft against Garrett and Able; (7) Breach of Fiduciary Duty against Garrett; (8) Conversion against Garrett; and (9) violation of the CFAA against Garrett and Able. (Am.Compl. pp. 16–26.)

III. ANALYSIS

*4 Defendant Garrett’s Motion seeks dismissal of Plaintiff’s CFAA claim and argues that the Amended Complaint fails to state a claim upon which relief could be granted. (ECF No. 196.) Defendant Able’s Motion raises this same argument and also alleges that: (1) once the CFAA claim is dismissed, the Court should decline to exercise supplemental jurisdiction over the remaining state law claims; (2) the Court should decline to exercise jurisdiction over this action under the *Colorado River* doctrine; and (3) Plaintiff’s Amended Complaint fails to state a claim with respect to three of the state law claims. (ECF No. 217.) The Court will address each of these issues in turn below.

A. CFAA Claim

Both Garrett and Able allege that Plaintiff’s Amended Complaint fails to state a claim for violation of the CFAA. The CFAA provides, in pertinent part, that it shall be unlawful for anyone to “intentionally access[] a protected computer without authorization and as a result of such conduct, cause[] damage and loss.” 18 U.S.C. § 1030(a)(5)(C). Therefore, to state a claim under this subsection, Plaintiff must allege that Defendants: (1) intentionally accessed a protected computer; (2) without authorization; and (3) caused damage or loss. *Id.* Defendants dispute the second prong of this claim and argue that, because Garrett was authorized to access the laptop while he was employed by Plaintiff, he cannot have accessed the laptop without authorization. (ECF No. 217 at 6.)

The Tenth Circuit has yet to address what constitutes “unauthorized access” for purposes of the CFAA and there is a split in the circuits. In *International Airport Centers, LLC v. Citrin*, 440 F.3d 418 (7th Cir.2006), the

defendant was employed by the plaintiff and had a company-issued laptop. Defendant decided to quit his employment and go into business for himself. Before he returned his employer-provided laptop, he installed a “secure-erasure program” that deleted all of the data on the laptop and made it unrecoverable. The Seventh Circuit held that the loading of the secure-erasure program onto the laptop constituted unauthorized “damage” or to the laptop and violated the CFAA. *Id.* at 419. Using agency principles, the court rejected defendant’s contention that his access was not unauthorized because he was an employee:

[Defendant’s] authorization to access the laptop terminated when, having already engaged in misconduct and decided to quit IAC in violation of his employment contract, he resolved to destroy files that incriminated himself and other files that were also the property of his employer, in violation of the duty of loyalty that agency law imposes on an employee.

...

“Violating the duty of loyalty, or failing to disclose adverse interests, voids the agency relationship.” *State v. DiGiulio*, 172 Ariz. 156, 835 P.2d 488, 492 (App.1992). “Unless otherwise agreed, the authority of the agent terminates if, without knowledge of the principal, he acquires adverse interests or if he is otherwise guilty of a serious breach of loyalty to the principal.” *Id.*

*5 *Id.* at 420 (internal citations omitted). Therefore, under the Seventh Circuit’s approach, whether access to a computer was “unauthorized” depends on the status of the agency relationship between the employer and employee.

Other circuits have taken a more narrow view on what constitutes “unauthorized access” for purposes of the CFAA. In *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127 (9th Cir.2009), the Ninth Circuit held:

The plain language of the statute therefore indicates that “authorization” depends on actions taken by the employer. Nothing in the CFAA suggests that a defendant’s liability for accessing a computer without authorization turns on whether the defendant breached a state law duty of loyalty to an employer. If the employer has not rescinded the defendant’s right to use the computer, the defendant would have no reason to know that

making personal use of the company computer in breach of a state law fiduciary duty to an employer would constitute a criminal violation of the CFAA.

Id. at 1135. Thus, the Ninth Circuit's approach focuses on whether the employer has specifically rescinded the employee's access to the computer in determining whether such access was "unauthorized."

As previously stated, the Tenth Circuit has not yet taken a position on this issue. However, the split in circuits is immaterial to this case because under either standard Plaintiff's Amended Complaint states a claim. SBM informed Garrett that he was required to return all property that he had been given, including his equipment, at the time he ended his employment. (Am.Compl.¶ 37.) Thus, SBM explicitly revoked Garrett's access to the laptop as of his last day as an employee. Garrett failed to return much of his equipment, including a laptop, on his last day and canceled a follow-up meeting SBM had scheduled to collect this equipment. (*Id.* ¶ 38.) Garrett retained the laptop for approximately three weeks after he terminated his employment with Plaintiff. (*Id.* ¶ 39.) When he returned the laptop to Plaintiff, it had been "intentionally erased." (*Id.*) The Court finds that it is reasonable to infer that Garrett accessed the laptop after his last day of employment with SBM or, stated differently, it is unreasonable to infer that Garrett retained the SBM laptop for about three weeks after his employment with SBM had terminated only to refrain from accessing said laptop during this prolonged period of time. As a consequence, the Court holds that SBM has stated a claim for violation of the CFAA.

The cases cited by Defendants for the proposition that Garrett's access to the laptop was not "unauthorized" are easily distinguishable because they involve the use (or alleged misuse) of company-provided equipment during the duration of the defendant's employment. *See, e.g., Shamrock Foods Co. v. Gast*, 535 F.Supp.2d 962, 967 (D.Ariz.2008) (employee did not violate CFAA by emailing himself information during his employment that he was authorized to access); *Diamond Power Intern., Inc. v. Davidson*, 540 F.Supp.2d 1322, 1343 (N.D.Ga.2007) (employee that downloaded confidential data onto a zip drive during his employment did not violate CFAA). In this case, Garrett retained Plaintiff's laptop for three weeks *after his employment ended*, including more than two weeks after he started his employment with Able, a direct competitor with SBM. (Am.Compl.¶¶ 37-41.)

*6 There can be no question that, under either the Seventh or the Ninth Circuit's interpretation of "unauthorized access", Garrett's access to the laptop became unauthorized when his employment ended and SBM requested return of the laptop. Therefore, the Court finds that the Amended Complaint states a claim for violation of the CFAA against Garrett.

The Court also finds that the Amended Complaint states a claim for a CFAA violation against Able. Garrett began his employment with Able on January 28, 2010. (Am.Compl.¶ 41.) At such time, Garrett became an agent of Able and Able became liable for any actions taken within the scope of his employment. *See Stat-Tech Liquidating Trust v. Fenster*, 981 F.Supp. 1325, 1336 (D.Colo.1997). Garrett did not return the laptop computer to Plaintiff until more than two after he began his employment with Able. (Am.Compl.¶ 39.) It is reasonable to infer that Garrett accessed SBM's laptop during the time that he was employed with Able and in the scope of such employment. Plaintiff's Amended Complaint therefore states a claim for violation of the CFAA against Able. *See Shurgard Storage Ctrs, Inc. v. Safeguard Self Storage*, 119 F.Supp.2d 1121, 1125 (W.D.Wash.2000) (holding that complaint by former employer stated a claim for violation of CFAA against new employer under agency theory); *Charles Schwab & Co., Inc. v. Carter*, 2005 WL 2369815, *7 (N.D.Ill. Sept. 27, 2005) (new employer liable for violation of CFAA where new employer affirmatively urged employee to access former employer's computer system).

Accordingly, Defendants' Motions are denied to the extent they seek dismissal of Plaintiff's CFAA claim against both Defendants.

B. Supplemental Jurisdiction

Defendant Able argues that, if Plaintiff's CFAA claim is dismissed, the Court should decline to exercise supplemental jurisdiction over Plaintiff's state law claims pursuant to 28 U.S.C. § 1367. However, because the Court finds that Plaintiff has stated a claim for violation of the CFAA, the Court finds no just cause to decline supplemental jurisdiction over the state law claims. Accordingly, Able's Motion to Dismiss is denied to the extent it asks the Court to decline supplemental jurisdiction over Plaintiff's state law claims.

C. Colorado River Doctrine

Able also argues that the Court should decline to exercise jurisdiction over this case pursuant to the *Colorado River*

doctrine because there is parallel litigation ongoing in the California state courts ("California Action"). (ECF No. 217 at 10–11.)

The *Colorado River* doctrine governs whether a district court should stay or dismiss a federal suit pending the resolution of a parallel state court proceeding. See *Colorado River Water Conservation Dist. v. United States*, 424 U.S. 800, 817–18 (1976). The Supreme Court has held that federal courts may not use any of the abstention doctrines to refuse to exercise jurisdiction over a suit for non-equitable relief that duplicates an ongoing state litigation. See *Colorado River*, 424 U.S. at 813, 816–818. However, the Supreme Court also concluded that judicial economy concerns may justify deferral of a federal suit when pending state litigation will resolve the issues presented in the federal case. See *id.* at 817–20. Under the abstention doctrines, the Court is required to abstain in many circumstances; however, whether to decline to exercise jurisdiction pursuant to *Colorado River* is discretionary. *Rienhardt v. Kelly*, 164 F.3d 1296, 1303 (10th Cir.1999).

*7 The Tenth Circuit has warned that the appropriate circumstances for deferral under the *Colorado River* doctrine are "considerably more limited than the circumstances appropriate for abstention" and must be "exceptional." *Id.* (quoting *Colorado River*, 424 U.S. at 817–18). Accordingly, the Court's "task in cases such as this is not to find some substantial reason for the exercise of federal jurisdiction ...; rather, the task is to ascertain whether there exist exceptional circumstances, the clearest of justifications, that can suffice under *Colorado River* to justify the surrender of the jurisdiction." *Id.* (quoting *Moses H. Cone Memorial Hosp. v. Mercury Constr. Corp.*, 460 U.S. 1, 25–26 (1983)). Simply stated, "[d]espite the temptation for federal courts to use the doctrine as a means of stemming the rising tide of litigation, suits in federal court are not easily swept away by *Colorado River*." *Id.*

The first step under the *Colorado River* analysis is determining "whether the state and federal proceedings are parallel." *Allen v. Board of Educ., Unified Sch. Dist.*, 436, 68 F.3d 401, 403 (10th Cir.1995). Suits are parallel if "substantially the same parties litigate substantially the same issues in different forums." *Id.* The court examines "the state proceedings as they actually exist to determine whether they are parallel to the federal proceedings, resolving any doubt in favor of exercising federal jurisdiction." *Id.* If the cases are not parallel, the federal court must exercise jurisdiction. *Allen*, 68 F.3d at 403. If the cases are parallel, the federal court must consider a multitude of other factors in deciding whether to

surrender jurisdiction until the conclusion of state court proceedings. *Id.*

The nature of the parties and the claims raised in his case is set forth above. The California Action was filed by Able against SBM in San Francisco Superior Court seeking a declaratory judgment on the following issues: (1) the enforceability Noncompetition Agreement between Garrett and SBM; (2) to which of SBM's protectable trade secrets Able allegedly has access; (3) whether Able misappropriated any of SBM's trade secrets; (4) whether SBM violated California Business and Professions Code § 17200 *et seq.*; and (5) whether SBM violated California Penal Code § 502. (ECF No. 217–5.) SBM cross-claimed against Able and three of its executives alleging that they violated California's Uniform Trade Secret Act and California Business and Professions Code § 17200. (ECF No. 217–4.)

Able claims that this case is parallel to the California Action because they involve substantially the same issues and parties. The Court disagrees. There are at least three additional defendants named in the California Action who are not parties to this case. Perhaps more significantly, it is unclear whether Garrett is a party to the California Action.¹ Additionally, there are material differences in the claims pled in the two actions. The instant action brings two Colorado statutory claims and the CFAA claim, none of which are part of the California Action. This case also involves six common law claims as to which the Court has not had the occasion to determine whether California or Colorado law applies.² The California Action is a declaratory judgment action which involves at least two California statutes and omits many of the common law claims pled in this action. Given these material differences in the claims asserted in the respective cases, the Court finds that the two actions are not parallel.

*8 Moreover, even if the Court were to assume that the actions were parallel, it would not be compelled to decline jurisdiction over this case. The Supreme Court has identified several non-exclusive factors to consider in evaluating whether to decline jurisdiction, including: (1) whether the state or federal court has assumed jurisdiction over property in dispute; (2) the inconvenience to the parties of the federal forum; (3) avoiding piecemeal litigation; (4) the order in which the courts obtained jurisdiction; (5) the vexatious nature of the litigation; (6) whether federal law provides the rule of decision; and (7) and the adequacy of the state court proceeding to protect the federal plaintiff's rights. See *Colorado River*, 424 U.S. at 818; *Moses H. Cone*, 460 U.S. at 18–28. These factors are not a "mechanical checklist"; rather, the Court should "careful[ly] balanc[e] ... the most important factors as they apply in a given case, with the balance heavily

SBM Site Services, LLC v. Garrett, Not Reported in F.Supp.2d (2012)

weighted in favor of the exercise of jurisdiction.” *Fox v. Maulding*, 16 F.3d 1079, 1082 (1994).

Probably the most significant factor in this case is the order in which the respective courts obtained jurisdiction. Able contends that this factor weighs in favor of declining to exercise jurisdiction because it was involved in the California Action before it became a party to this case. (ECF No. 217 at 12.) The Court acknowledges that Able was not named as a party in this action until nine days after the California case commenced; however, at the time Able was added as a Defendant, this action had already been pending for nine months. Therefore, this Court already had jurisdiction over SBM and Garrett and the majority of the claims at issue in the two cases nine months before the matter was before the California court.

Additionally, the Supreme Court has held that this factor “should not be measured exclusively by which complaint was filed first, but rather in terms of how much progress has been made in the two actions.” *Moses H. Cone*, 460 U.S. at 21. In a motion filed in the California Action asking the California court to stay that proceeding, Able stated that “[t]he Colorado action has progressed far more rapidly than the California state court action” and admitted that the litigation posture of this action was far more advanced than the California Action. (ECF No. 558–3 at 7–8.) Indeed, the docket for this case is rapidly approaching six hundred entries. Magistrate Judge Boyd N. Boland has spent an extraordinary amount of time working with the parties to resolve evidentiary and discovery-related disputes. He has held a multitude of hearings, including a two-day hearing on Plaintiff’s Motion for Preliminary Injunction. (ECF Nos. 328 & 329.) Magistrate Judge Boland has made a number of factual findings, including the following: (1) certain SBM documents constitute trade secrets; (2) Garrett used improper means to acquire SBM’s trade secrets; (3) Able acquired SBM’s trade secrets from Garrett; and (4) these trade secrets were obtained in violation of Garrett’s Confidentiality Agreement. (ECF No. 364 at 17–18.) Magistrate Judge Boland has entered an injunction barring Garrett and Able from possessing SBM trade secret information and ordering them to return any trade secret information in their possession. (*Id.*)

*9 From what the Court can discern, the California Action appears to have only recently entered the discovery phase. Neither party has cited any substantive rulings made by the California court. Thus, even though the California court had jurisdiction over Able nine days before this Court, the fact that this case is far more advanced than the California Action weighs heavily in favor of this Court exercising jurisdiction over the above-captioned action.

Able also contends that the Court should decline jurisdiction because SBM engaged in forum shopping in choosing to file this action in Colorado. Able alleges that it was not originally named as a party because SBM wanted to “skirt[] the issue of jurisdiction.” (ECF No. 321 at 11.) However, jurisdiction in this case is not predicated on diversity; SBM brings a federal claim against Defendants. Because Garrett lives in Colorado, SBM could have brought this action here regardless of whether Able was named as a party from the outset. *See* 28 U.S.C. § 1391(b). The Court sees nothing vexatious about SBM choosing to file this action against Garrett in Colorado and then later adding Able as a party after it learned, through discovery, of the timing of events with respect to when Garrett began his employment with Able.

In fact, if either of these actions are vexatious, it appears more likely that the California Action would qualify as forum shopping. Able contends that, because it was not originally named in this action, it “had no choice other than to file the state court action to force SBM to disclose what trade secrets it claimed were stolen by Able.” (ECF No. 321 at 11.) But Able could have sought to intervene or otherwise joined in this action. Also, in a hearing in the California Action, Able admitted that part of its motivation in bringing its claims against SBM in California state court was that Colorado’s laws are not “quite as protective” as those in California. (ECF No. 556–2³ at 6.) Thus, the Court finds that the vexatious nature of Able’s litigation tactics weighs in favor of it exercising and retaining jurisdiction over this case.

Able also contends that the California court is more convenient. (ECF No. 217 at 12.) Because SBM and Able are based in California, the California court is likely somewhat more convenient. But the principal actor in this case—Garrett—lives in Colorado and many of Garrett’s allegedly wrongful acts occurred in Colorado. Able has hired counsel in Colorado and admitted in a filing in the California Action that “Colorado is a suitable place for trial.” (ECF No. 558–3 at 8.) Thus, the convenience advantage of the California court does not carry significant weight in this analysis.

In sum, the Court has carefully balanced the factors set forth in *Colorado River* and *Moses H. Cone* and finds that this is not an “exceptional” case that warrants declining to exercise jurisdiction. Accordingly, Able’s Motion to Dismiss is denied to the extent it asks the Court to dismiss this action under the *Colorado River* doctrine.

D. Inevitable Disclosure Claim

SBM Site Services, LLC v. Garrett, Not Reported in F.Supp.2d (2012)

*10 The fourth claim for relief in Plaintiff's Amended Complaint seeks an injunction to prevent Garrett from working for Able under the "inevitable disclosure" doctrine. (ECF No. 190 ¶¶ 70–80.) Able moves to dismiss this claim and argues that California law does not recognize such a claim. (ECF No. 217 at 13.) In its recently-filed supplemental briefing, SBM states: "SBM's inevitable disclosure claim has been rendered moot as to Able by the termination of Garrett's employment with Able. Simply put, the Court cannot enjoin Garrett from working for Able if he no longer works for Able." (ECF No. 558 at 4.)

The Court construes SBM's statements in its recent filing as a withdrawal or voluntary dismissal of its inevitable disclosure claim. Accordingly, Able's Motion to Dismiss is denied as moot with respect to Plaintiff's inevitable disclosure claim as such claim has been withdrawn.

E. Misappropriation of Trade Secrets

Plaintiff's fifth claim for relief alleges that Able and Garrett misappropriated trade secrets in violation of Colo.Rev.Stat. § 7–74–101 *et seq.* (Am.Compl.¶¶ 81–89.) Able moves to dismiss this claim and argues that SBM has not alleged with sufficient particularity which trade secrets it supposedly misappropriated. (ECF No. 217 at 14–15.)

Federal Rule of Civil Procedure 8(a)(2) requires only that a pleading include a "short, plain statement of the claim showing that the pleader is entitled to relief." Although some types of claims are subject to a heightened pleading standard that requires greater particularity, *see* Fed.R.Civ.P. 9, misappropriation of trade secrets is not such a claim. *See DSMC, Inc. v. Convera Corp.*, 273 F.Supp.2d 14, 24 (D.D.C.2002) (holding that the usual notice pleading requirements of Rule 8 apply to a trade secrets claim).

The cases rejecting trade secret claims for lack of specificity are predominantly at later stages in the litigation process. *See, e.g., Lear Siegler, Inc. v. Glass Plastics Corp.*, 1987 WL 15749 (N.D. Ill. Aug. 12, 1987) (granting summary judgment to defendant); *Composite Marine Propellers, Inc. v. Van Der Woude*, 962 F.2d 1263, 1266 (7th Cir.1992) (overturning jury verdict). Even the cases cited by Able in support of its argument are further along in the litigation than the motion to dismiss stage. *E.g., Knights Armament Co. v. Optical Sys. Tech., Inc.*, 254 F.R.D. 463, 467 (M.D.Fla.2008) (holding that a party must disclose which trade secrets were allegedly misappropriated during the discovery process). Courts have only dismissed a claim for lack of specificity

on the pleadings in the most extreme cases. *See, e.g., Thermal Zone Products Corp. v. Echo Eng., Ltd.*, 1993 WL 358148 at *5–6 (N.D.Ill. Sept. 14, 1993) (dismissing complaint that merely recited statutory language).

Paragraphs 45 and 46 of Plaintiff's Amended Complaint set forth specific documents and subjects of information that were allegedly misappropriated by Able and Garrett, including: "SBM's strategic plan which identifies SBM's strategy for doubling its facilities services business over a five-year period; ... SBM's historical bid information; sales power-points designed by SBM for particular customers." (Am.Compl.¶ 45.) The Court finds that these allegations contain sufficient detail to satisfy Rule 8's notice pleading requirement. Accordingly, Able's Motion to Dismiss is denied with respect to Plaintiff's misappropriation of trade secrets claim.

F. Civil Theft

*11 Plaintiff's sixth claim for relief alleges that Able and Garrett are liable for civil theft for having violated Colo.Rev.Stat. § 18–4–401 *et seq.* (Am.Compl.¶¶ 90–94.) Able moves to dismiss this claim and argues that it is preempted by Colorado's Uniform Trade Secrets Act ("CUTSA"), Colo.Rev.Stat. § 7–74–108. (ECF No. 217 at 16.)

This Court has rejected the contention that CUTSA was intended as a "blanket preemption to all claims that arise from a set of circumstances that happen to involve information that the plaintiff claims is in the nature of a trade secret." *Powell Prods., Inc. v. Marks*, 948 f.Supp. 1469, 1475 (D.Colo.1996). Instead, the Court has adopted a tailored approach in which only claims "restating the same operative facts as would plainly and exclusively spell out only trade secret misappropriation" are preempted. *Id.* at 1474. Thus, "the salient question in addressing the question of trade secrets act preemption is whether a challenged common law claim depends solely on a finding of trade secret status to be actionable. Where it does not, the claim is not preempted." *Virtual Cloud Servs., Inc. v. CH2M Hill, Inc.*, 2006 WL 446077, *2 (D.Colo. Feb. 21, 2006).

SBM contends that its civil theft claim is not preempted because it alleges that Able and Garrett misappropriated more than just trade secrets. (ECF No. 293 at 16.) In fact, Plaintiff's Amended Complaint alleges that Garrett has never returned "an external hard drive, the disk from Kieft, and copies of SBM's hard drive files." (Am.Compl.¶ 40.) This Court has held: "That portion of the conversion claim seeking recovery for stolen physical items such as blueprints and drawings would not be

SBM Site Services, LLC v. Garrett, Not Reported in F.Supp.2d (2012)

preempted because it would not be the subject of a misappropriation claim under the [C]UTSA.” *Virtual Cloud*, 2006 WL 446077, at *2. Because Plaintiff’s Amended Complaint alleges that, in addition to trade secrets, Able and Garrett stole actual physical items, the Court finds that its CUTSA claim is not preempted.

Accordingly, Able’s Motion to Dismiss is also denied to the extent it seeks dismissal of Plaintiff’s civil theft claim.

IV. CONCLUSION

For the reasons set forth above, the Court ORDERS the follow:

1. Defendant Garrett’s Partial Motion to Dismiss (ECF No. 196) is DENIED;
2. Defendant Able’s Motion to Dismiss (ECF No. 217) is DENIED;

Footnotes

- ¹ The copies of the pleadings from the California Action filed with the Court do not indicate that Mr. Garrett is a party to that action. (ECF Nos. 217–4 & 217–5.) However, Able has filed a transcript from a recent hearing in the California Action during which counsel stated that Garrett was now a party to that action. (ECF No. 556–2 at 9.) The Court takes judicial notice of this transcript. *See St. Louis Baptist Temple, Inc. v. Fed. Deposit Ins. Corp.*, 605 F.2d 1169, 1172 (10th Cir.1979) (federal courts may take notice of related proceedings in other courts).
- ² To the extent Able attempted to raise a choice of law question with respect to the entire case in its supplemental briefing, the Court finds that such efforts were procedurally improper. The Court granted the parties the opportunity to file supplemental briefing on the choice of law issue only to the extent that it was raised in the original Motions to Dismiss. Able’s Motion to Dismiss only raised choice of law with respect to SBM’s inevitable disclosure claim. (ECF No. 217 at 13.) Because, as discussed in section D below, Plaintiff concedes that its inevitable disclosure claim is now moot, the Court has no reason to make a finding regarding choice of law in ruling on the instant Motions. As a consequence, the Court GRANTS SBM’s Motion (ECF No. 559) to Strike Able’s Supplemental Brief (ECF No. 556) Regarding the Applicability of California Law or, in the Alternative, to Treat Able’s Supplemental Brief as a Motion for Partial Summary Judgment and Set Appropriate Briefing Schedule.
- ³ Although the Court has stricken Able’s Supplemental Brief Regarding Applicability of California Law, it takes judicial notice of the transcript from the California Action attached thereto. *See St. Louis Baptist Temple, Inc. v. Fed. Deposit Ins. Corp.*, 605 F.2d 1169, 1172 (10th Cir.1979) (federal courts may take notice of related proceedings in other courts).

3. Plaintiff has voluntarily withdrawn its Fourth Claim for Relief seeking an injunction under the Inevitable Discovery Doctrine and such claim is no longer pending in this action. Plaintiff’s Fourth Claim for Relief is thus DISMISSED WITHOUT PREJUDICE; and

4. Plaintiff’s Motion to Strike Able’s Supplemental Brief Regarding the Applicability of California Law or, in the Alternative, to Treat Able’s Supplemental Brief as a Motion for Partial Summary Judgment and Set Appropriate Briefing Schedule (ECF No. 559) is GRANTED; Defendant Able’s Supplemental Brief Regarding Applicability of California Law, ECF No. 556 is STRICKEN.

All Citations

Not Reported in F.Supp.2d, 2012 WL 628619